

FIG. 1

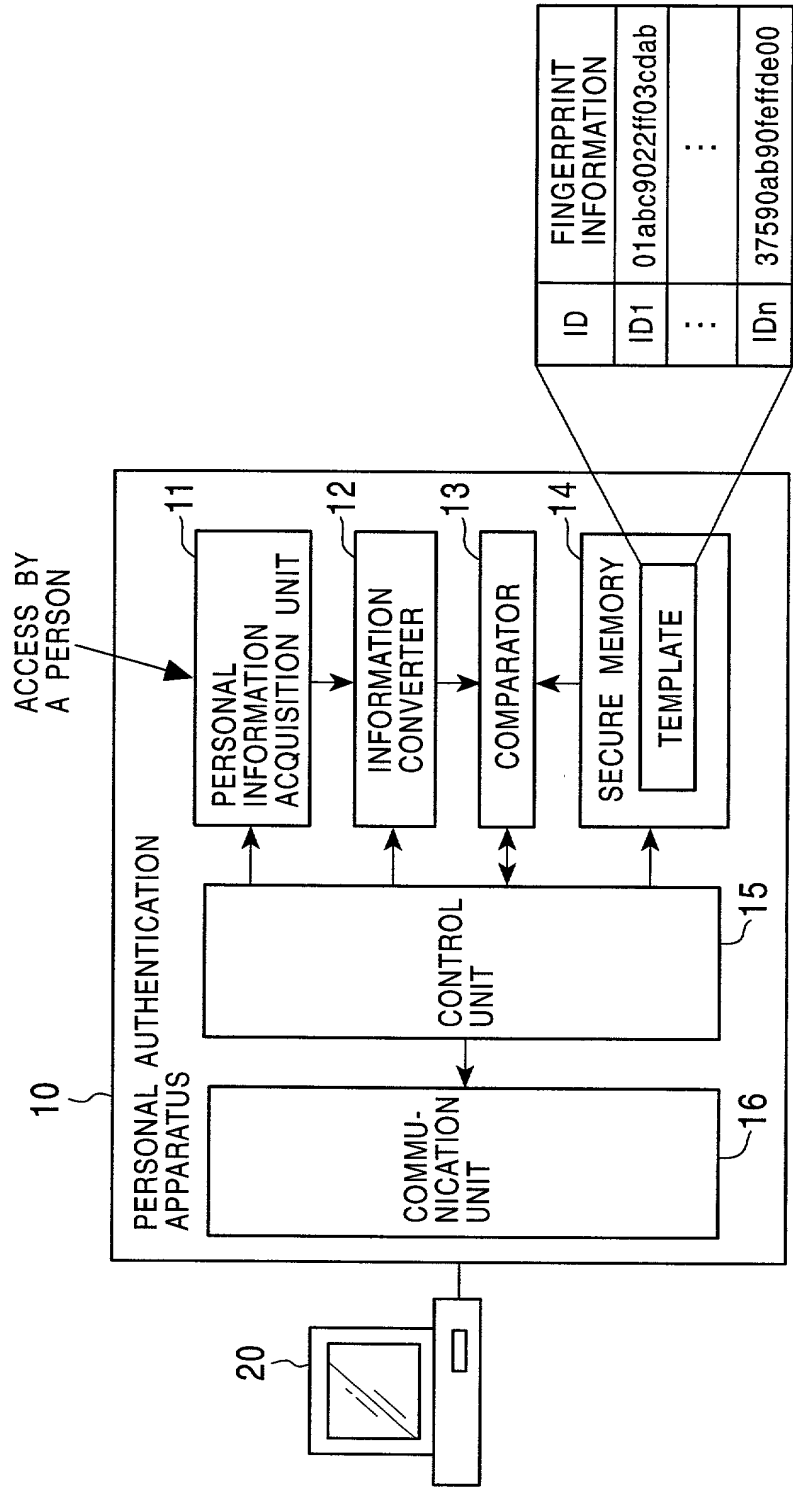


FIG. 2

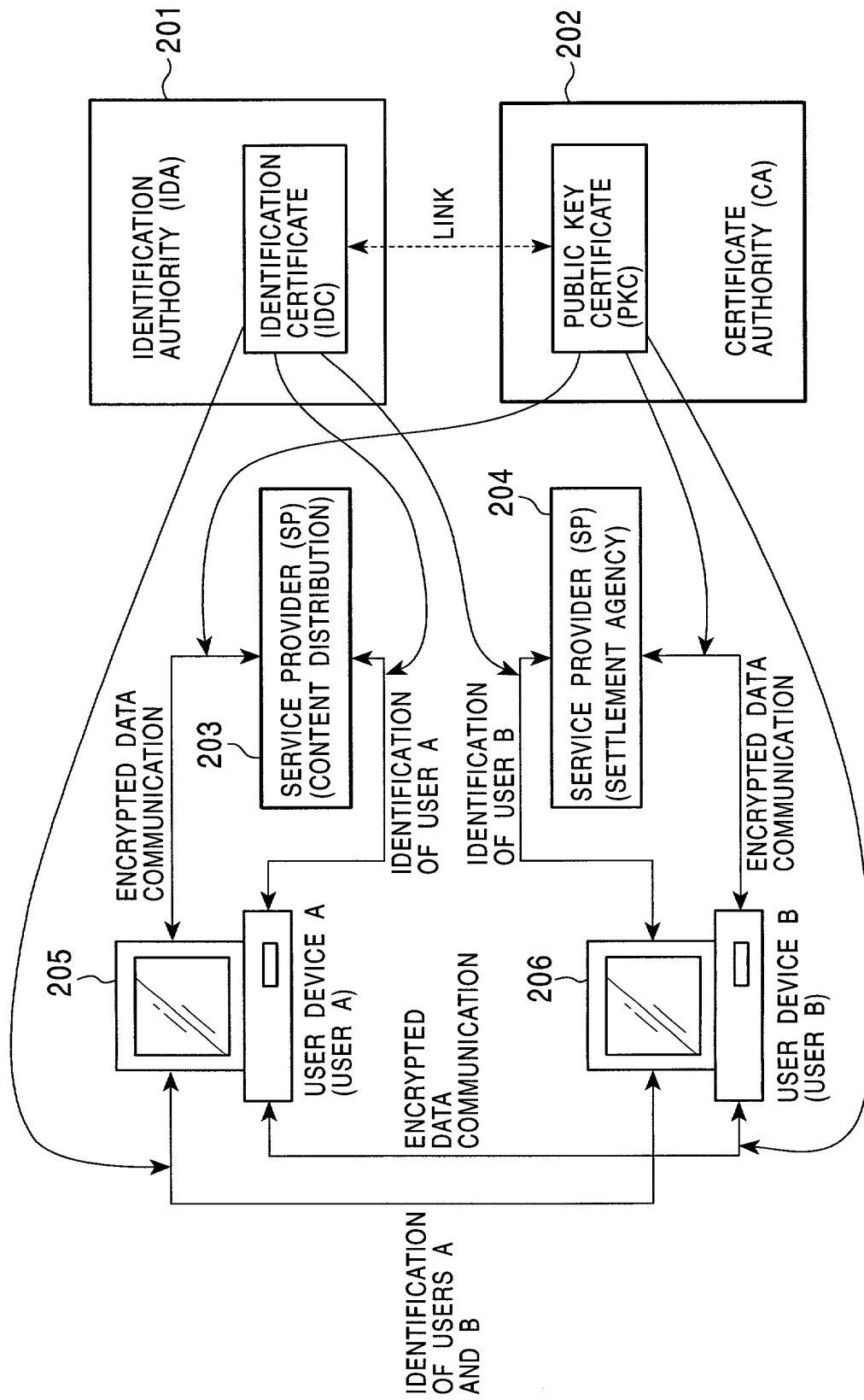


FIG. 3

Item	Description	Value employed in the present IA
Version 1		
version	Version of the certificate format	V3
serial Number	Serial number of the certificate assigned by the IA	Assigned in a serial fashion
signature algorithm Identifier algorithm parameters	Algorithm of the signature of the certificate and parameters thereof	Elliptic curve number/RSA parameters when an elliptic curve is used Key length when RSA is employed
issuer	IA name (in a distinguished name form)	Name of the present IA
validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date	
subject	Name which identifies the user	User device ID or ID of the service subject
subject Public Key Info algorithm subject Public key	Information of the public key of the user Algorithm of the key Key	Elliptic curve/RSA Public key of the user
Version 3		
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	Key identifier used in verification of the IA Key identification number (octal number) Name of the IA (in a general name form) Identification number	
subject key Identifier	Used when a plurality of keys are certified	Not used
key usage (0)digital Signature (1)non Repudiation (2)key Encipherment (3)data Encipherment (4)key Agreement (5)key CertSign (6)cRL Sign	Specifying the purpose of the key (0)for digital signature (1)to prevent repudiation (2)for encryption of the Key (3)for encryption of a message (4)for use in transmission of a symmetric key (5)used to verify the certificate (6)used to verify the signature of the certificate revocation list	0,1,4, or 6 is used
private Key Usage Period notBefore notAfter	Period during which the private key stored in the user is valid	Usage period is the same for the certificate, the public key, and the private Key (default)

FIG. 4

Certificate Policy policy Identifier policy Qualifiers	Certificate policy of the certificate authority Policy ID (according to ISO/IEC9834-1) Certification criteria	
policy Mappings issuer Domain Policy subject Domain Policy	Required only when the CA is certificated. Mappings of the policy of the issuer domain policy and the subject domain policy are defined	default = none
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	Attributes of the directory (X.500) are defined. Used to inform a receiving party of communication of the attributes the direction so that the receiving party can use the direction information	default = none
subject Alt Name	Alternative name of the user (in the form of GN)	not used
issuer Alt Name	Not used although this item is included in the certificate format (default = none)	default = none
subject Directory Attributes	Arbitrary attributes of the user	not used
basic Constraints	Specifies the public key to be certified	
ca path Len Constraint	Indicates whether the public key is used by a user or by a certificate authority to write a signature	default = used by a user
name Constraints permitted Subtrees base minimum	Used only when the certification is to certify a certification authority (CA)	default = none
maximum excluded Subtrees		
policy Constraints requier Explicit Policy inhibit Policy Mapping	Constraints are described in terms of requirements of explicit policy ID or inhibit policy mapping for the remaining certification path	
CRL Distribution Points	Indicates a reference point in the revocation list at which data is present which indicates whether the certificate of a user is revoked	Pointer which points to a location where the certificate is registered. The revocation list is managed by an issuer
Signature	Signature of the issuer	

FIG. 5

	Item	Description
Indispensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier algorithm parameters	Signature algorithm Algorithm Parameters
	Issuer	Name of the identification authority (in the form of a distinguished name)
	Validity notBefore notAfter	Period during which the certificate is valid Start date Expiration date
	Subject	Name of the subject to be certificated (in a DN form)
Extended Items	subject Template Info encrypt Type encrypt Unique ID  encryption Algorithm parameter validity subject Template Source subject Template	Template information <ul style="list-style-type: none"> <li>• encrypt Type</li> <li>• The unique ID or the certificate number of a public key certificate used for encryption</li> <li>• Algorithm</li> <li>• parameter</li> <li>• Validity period (start date, expiration date)</li> <li>• Type of the template</li> <li>• Template</li> </ul>
	Subject PKC info  subject PKC serial Number  subject PKC Unique ID	Information about the public key certificate of the subject <ul style="list-style-type: none"> <li>• Certificate number of the subject public key certificate</li> <li>• Unique ID of the subject of the subject public key certificate</li> </ul>
	Issuer Unique ID	Unique ID of the issuer
	Subject Unique ID	Unique ID of the subject
	Public Key Certificate	Public key certificate
	Issuer Alt Name	Alternative name of the issuer
	subject Directory Attributes	Personal information (encrypted as required) information used to authenticate subject Age, sex, etc.
	Valid Count	Number of times the certificate is allowed to be used
	Control Table Link Info Ctl Tbl Location Ctl Tbl Unique ID	Link information describing group information <ul style="list-style-type: none"> <li>• Location of a link information control table (URL, IP address, etc.)</li> <li>• Identification number of the link information</li> </ul>
Indispensable	IDA Signature	Signature of the IDA

FIG. 6A

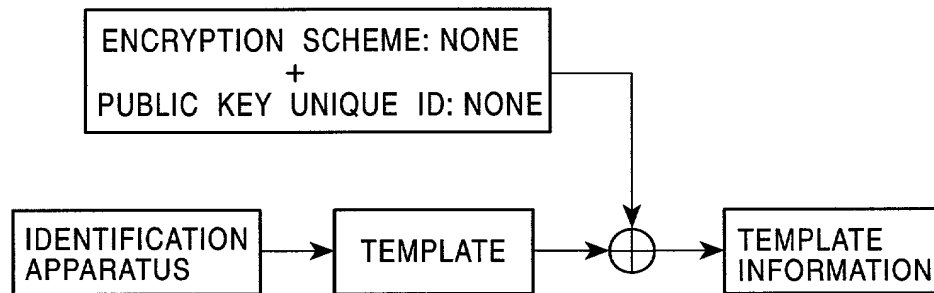


FIG. 6B

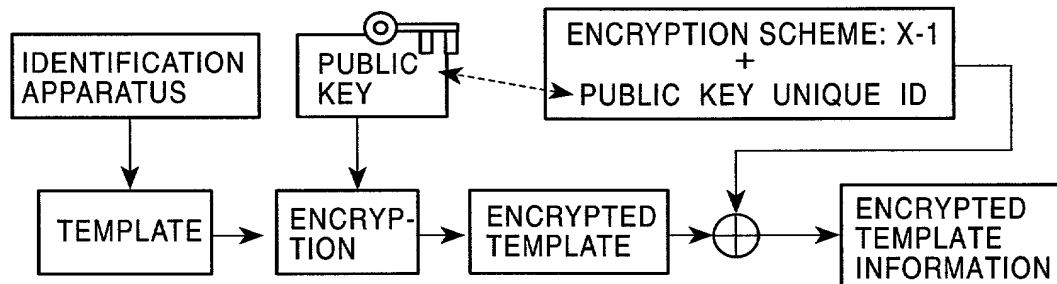


FIG. 6C

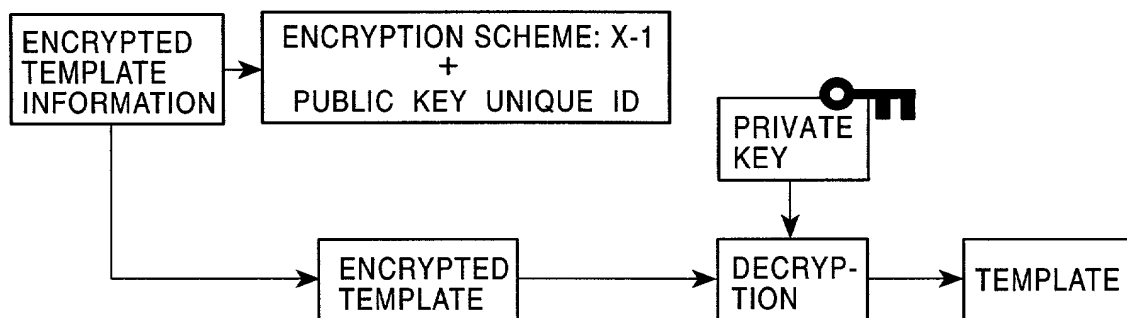


FIG. 7

PUBLIC KEY USED TO ENCRYPT TEMPLATES	EXAMPLES OF MANNERS IN WHICH TEMPLATE INFORMATION STORAGE IDC IS USED
PUBLIC KEY OF A USER OR A USER DEVICE	TO IDENTIFY AN AUTHORIZED USER OF A USER DEVICE (SUCH AS A PC) ON THE BASIS OF AN IDENTIFICATION CERTIFICATE OF THE USER
PUBLIC KEY OF A SERVICE PROVIDER	USED BY A SERVICE PROVIDER TO IDENTIFY A PARTICULAR USER SUCH AS A USER TO WHOM SERVICE IS TO BE PROVIDED, ON THE BASIS OF AN IDENTIFICATION CERTIFICATE (IDC) OF THE USER
PUBLIC KEY OF AN IDENTIFICATION AUTHORITY	IN DATA TRANSMISSION AMONG VARIOUS TERMINALS, A SENDER OR A RECEIVER IDENTIFIES

FIG. 8A

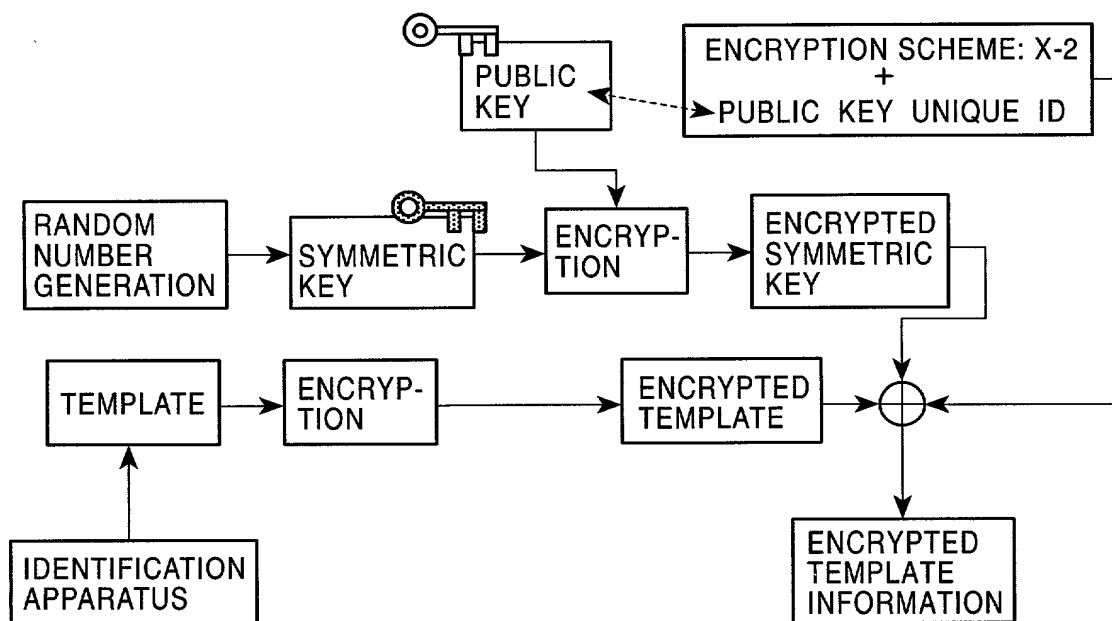


FIG. 8B

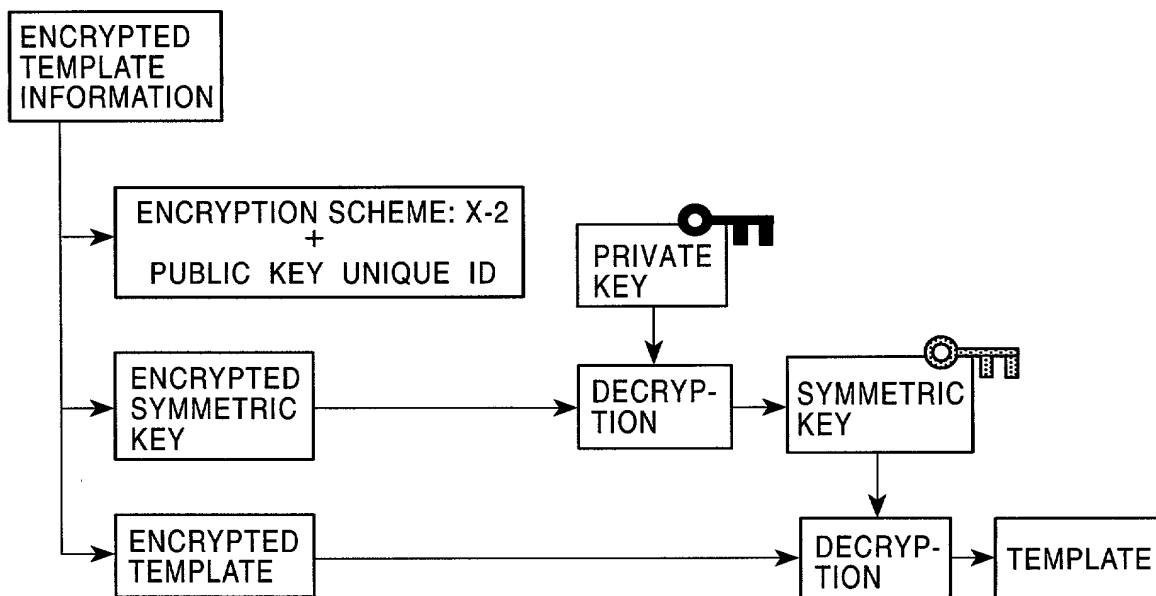




FIG. 9

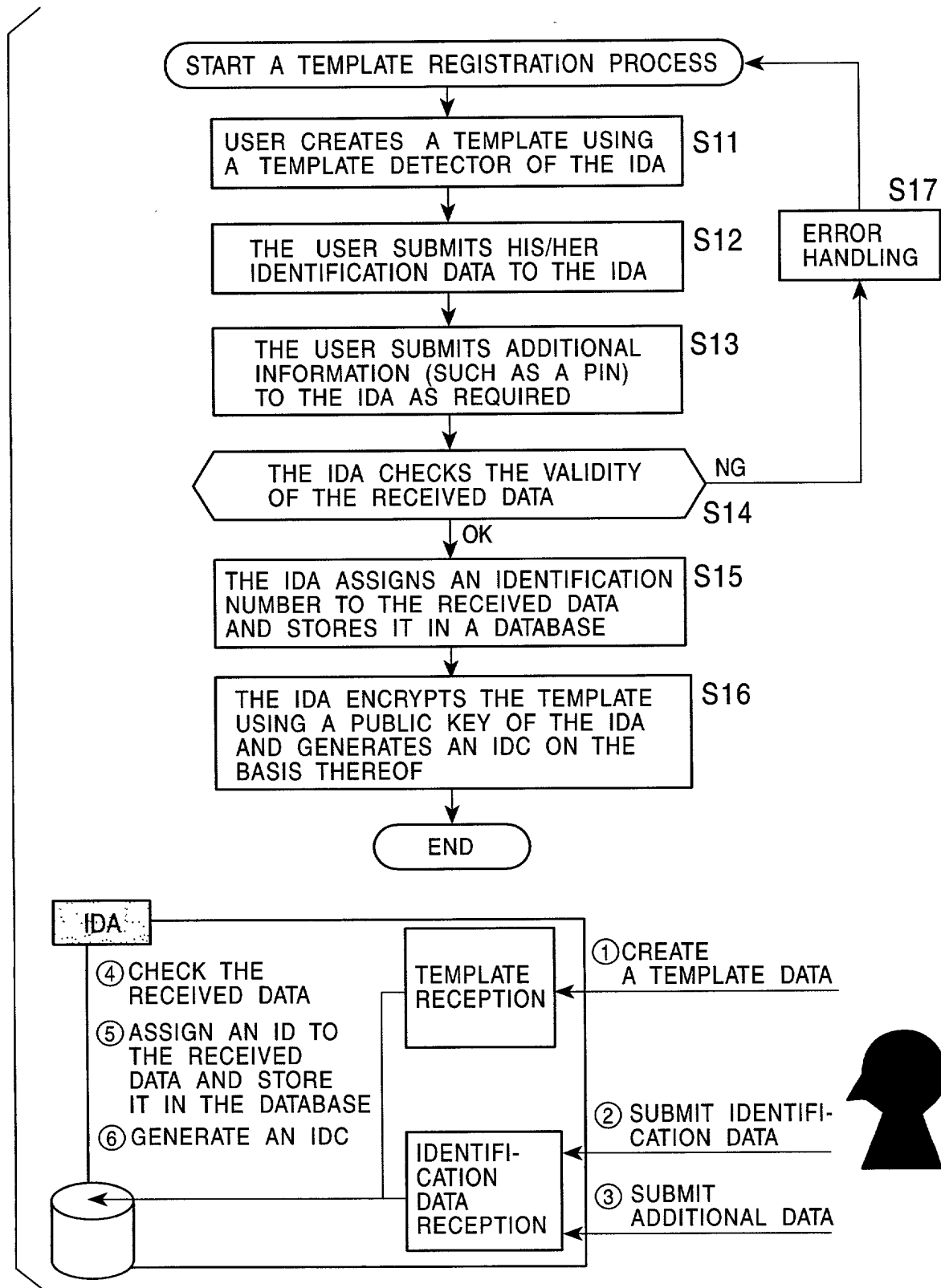


FIG. 10

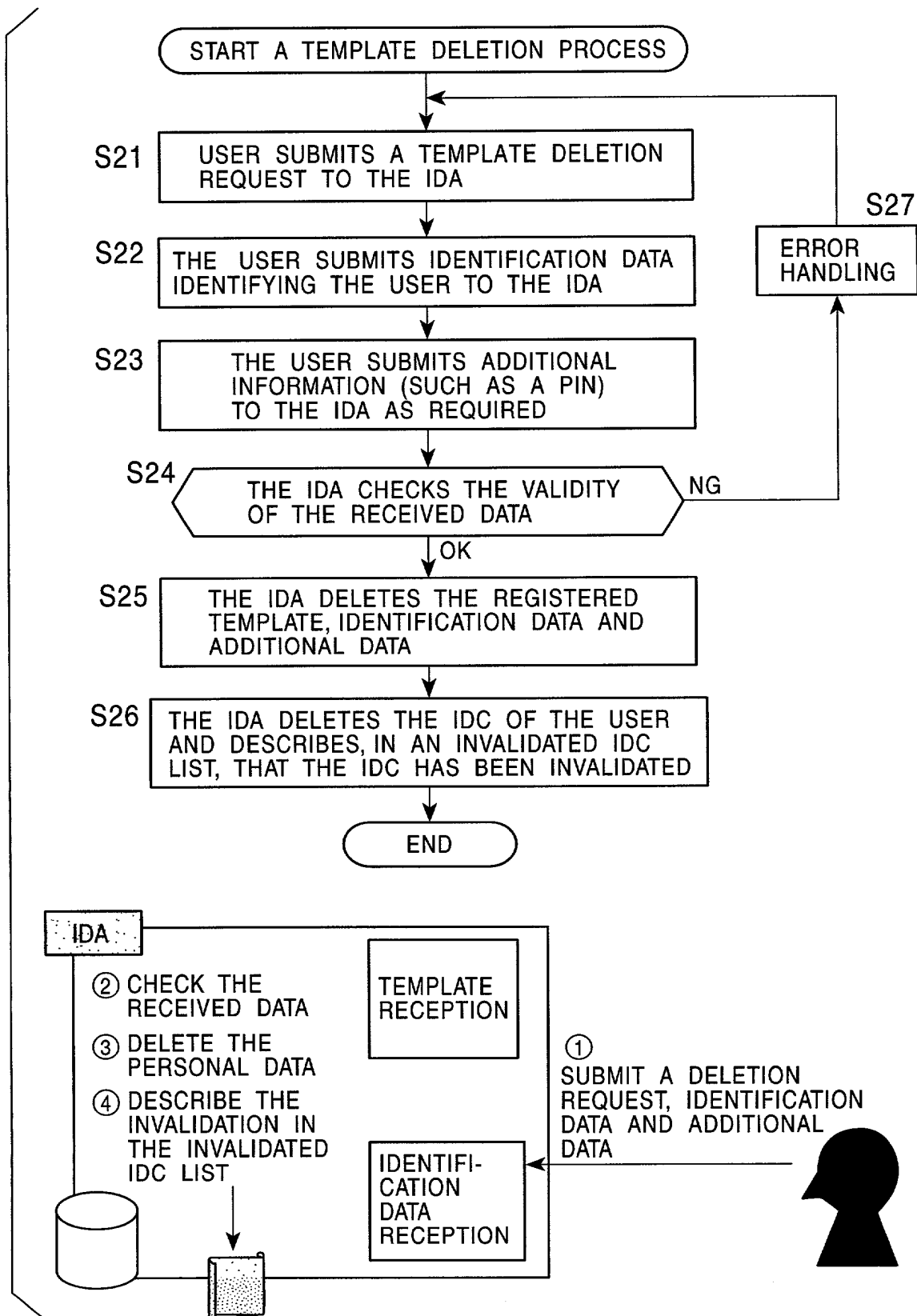


FIG. 11

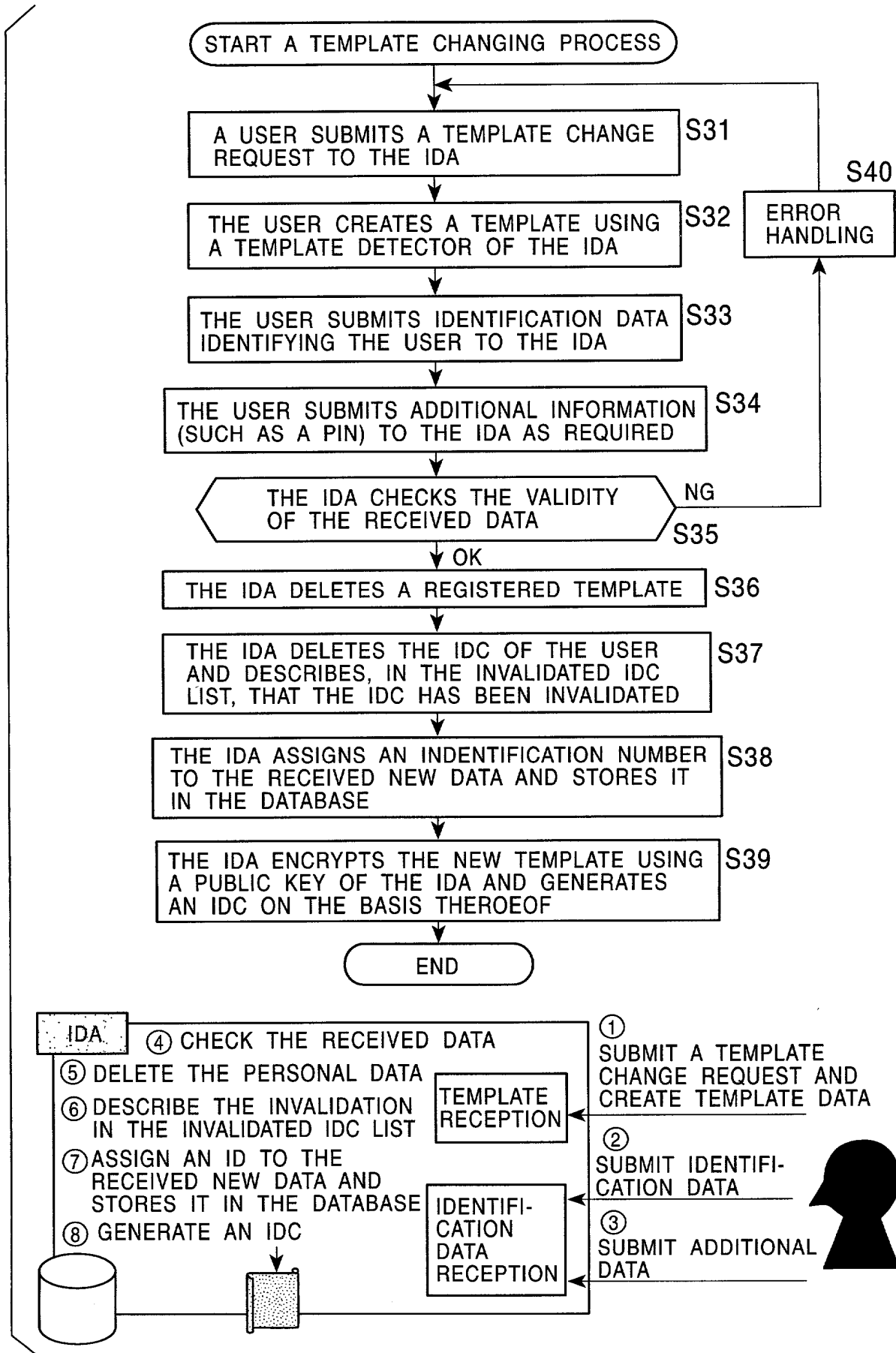


FIG. 12

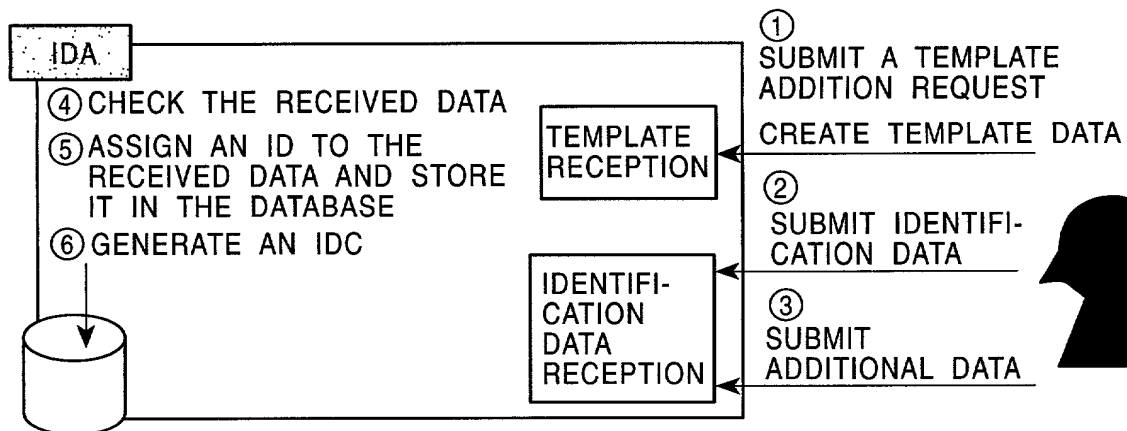
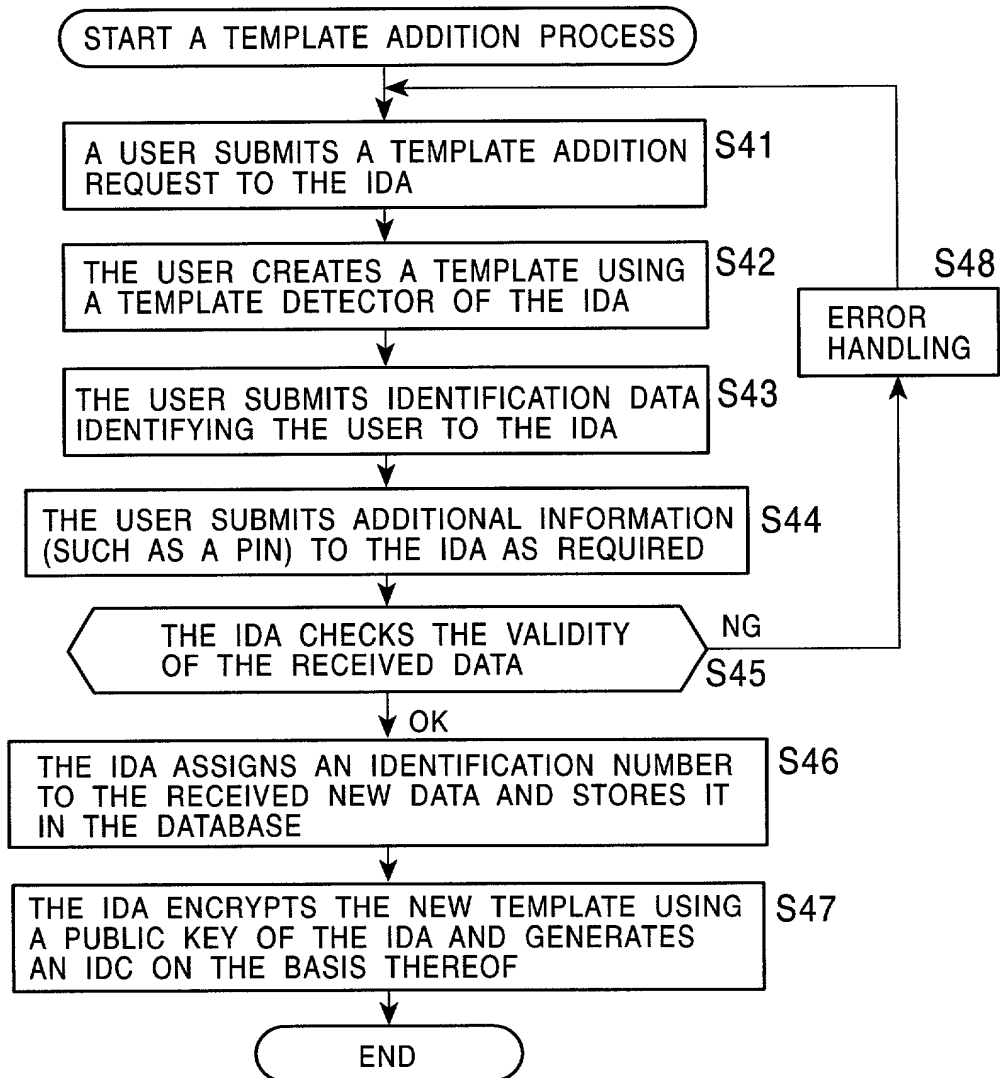


FIG. 13

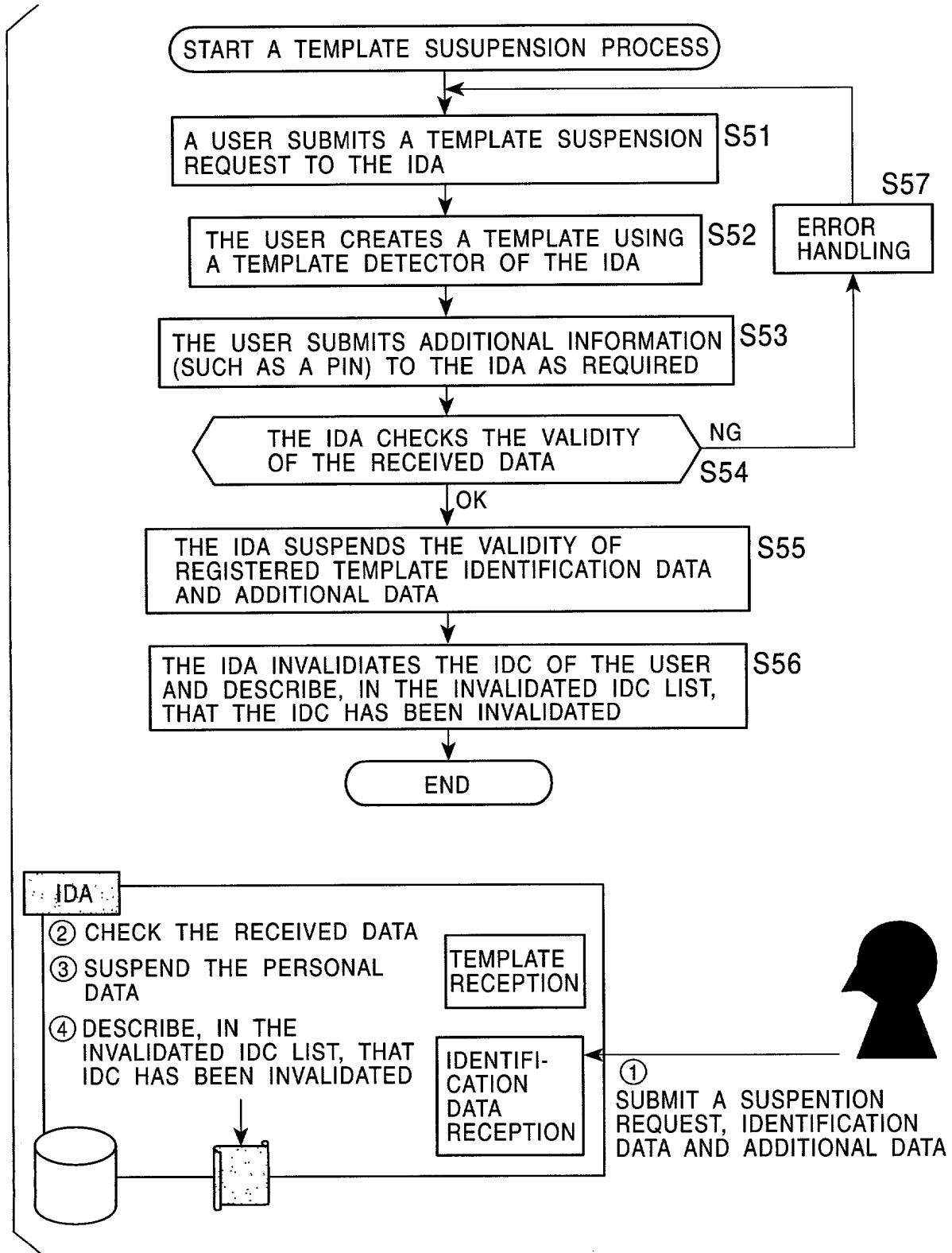


FIG. 14

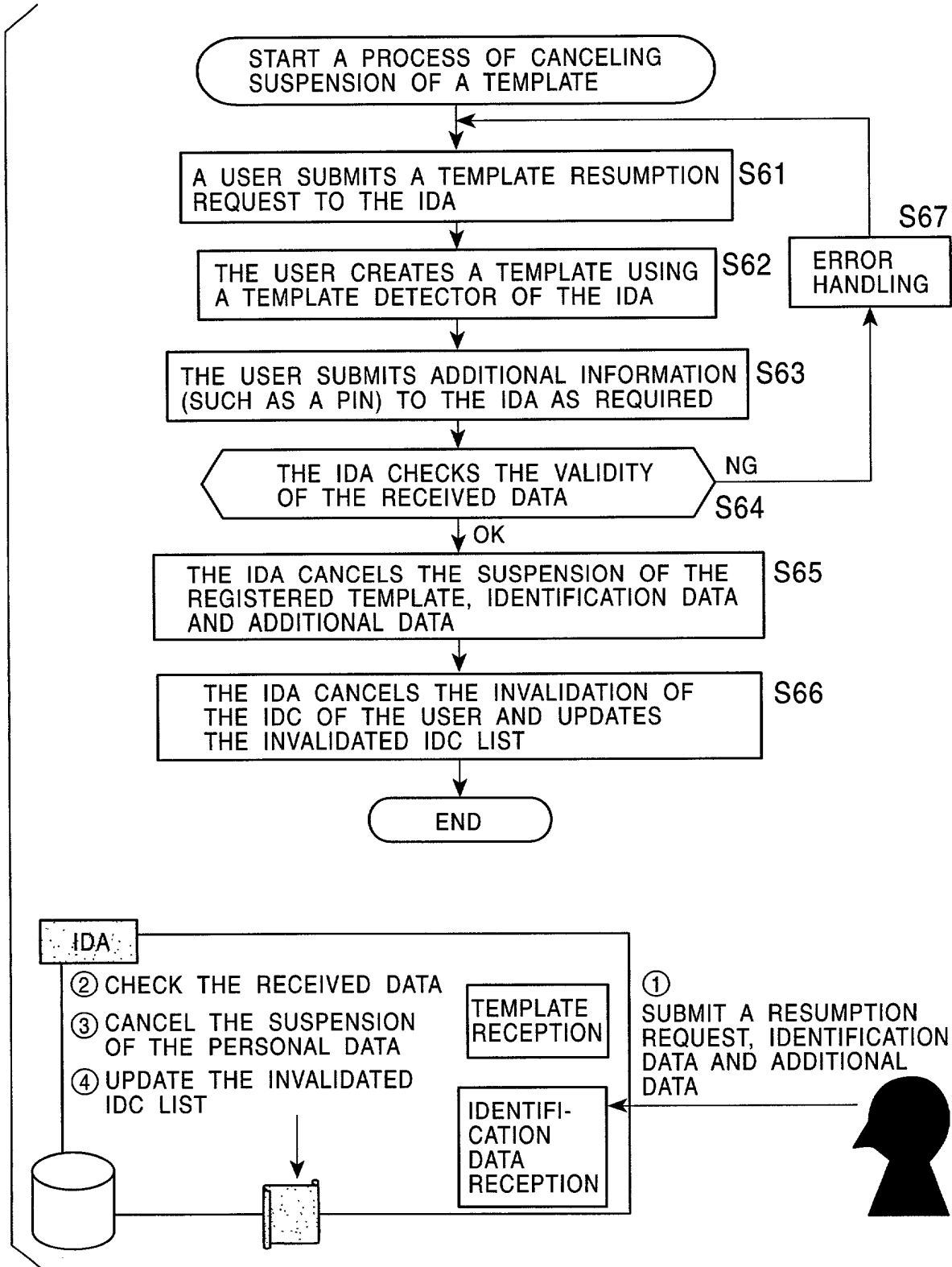


FIG. 15

15 / 89

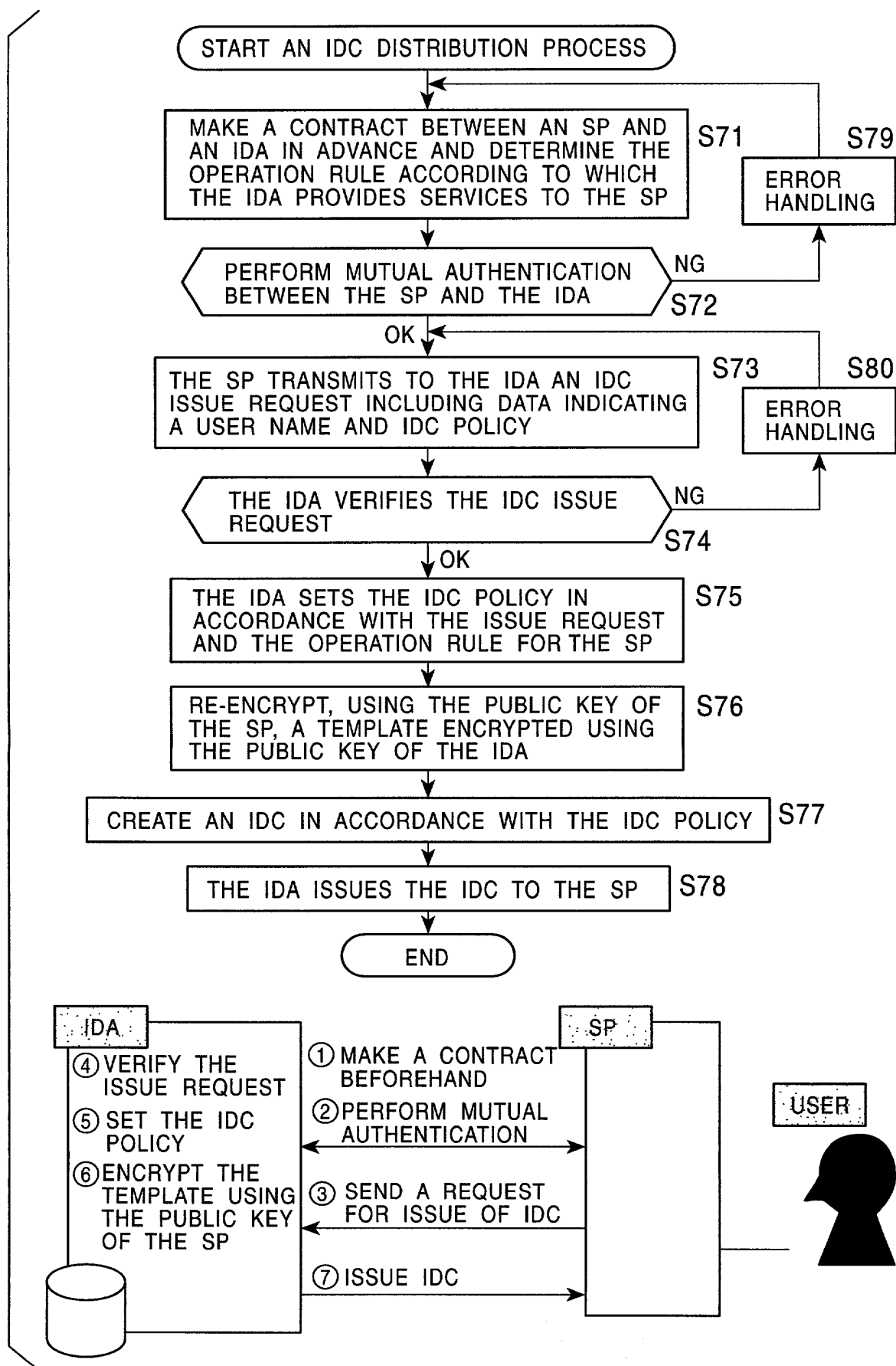


FIG. 16

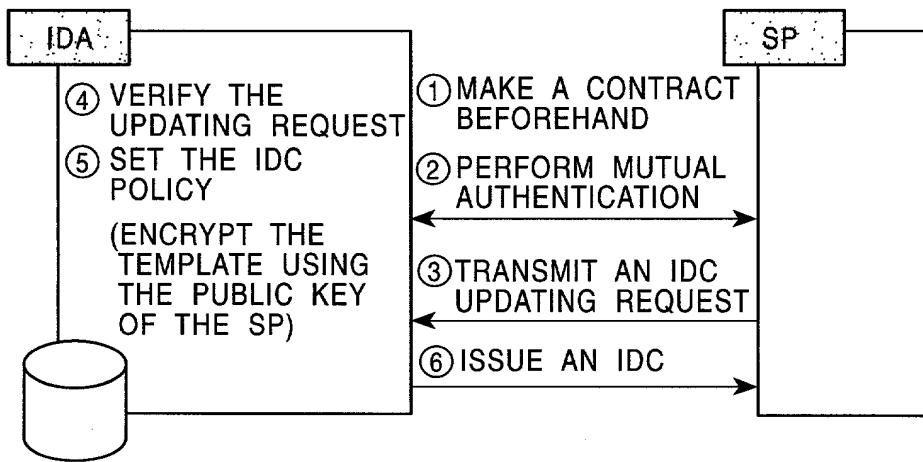
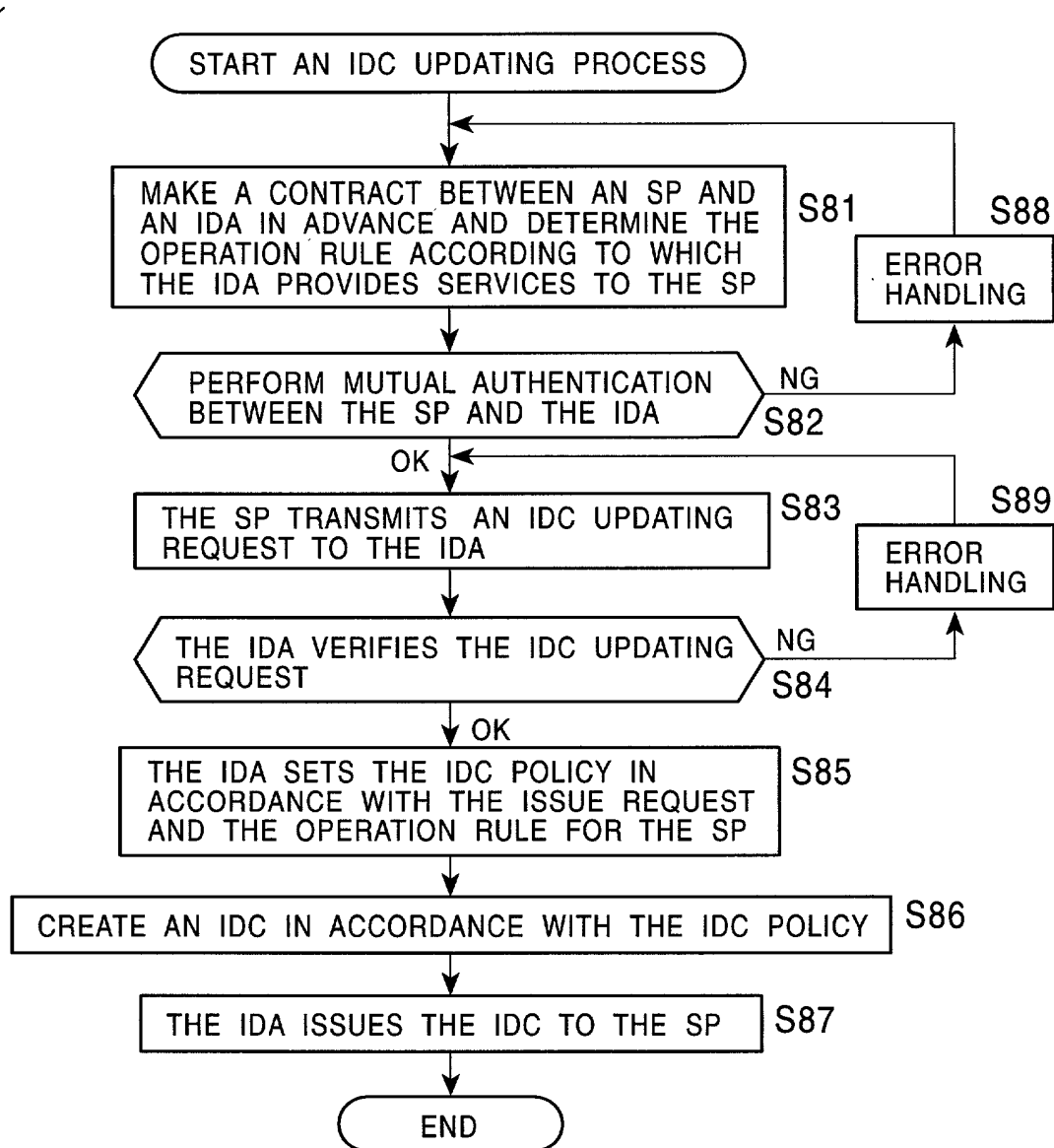




FIG. 17

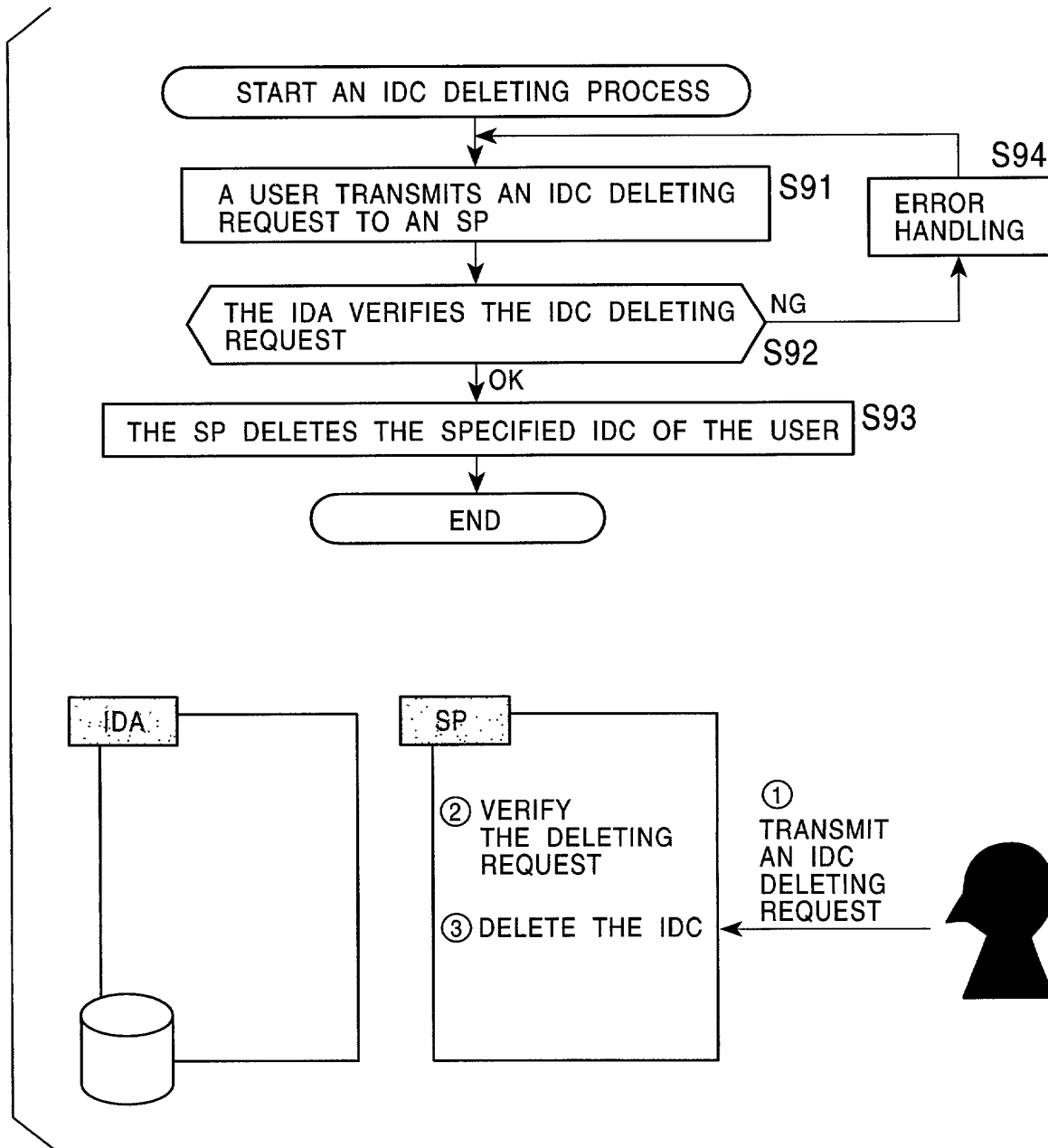


FIG. 18

18 / 89

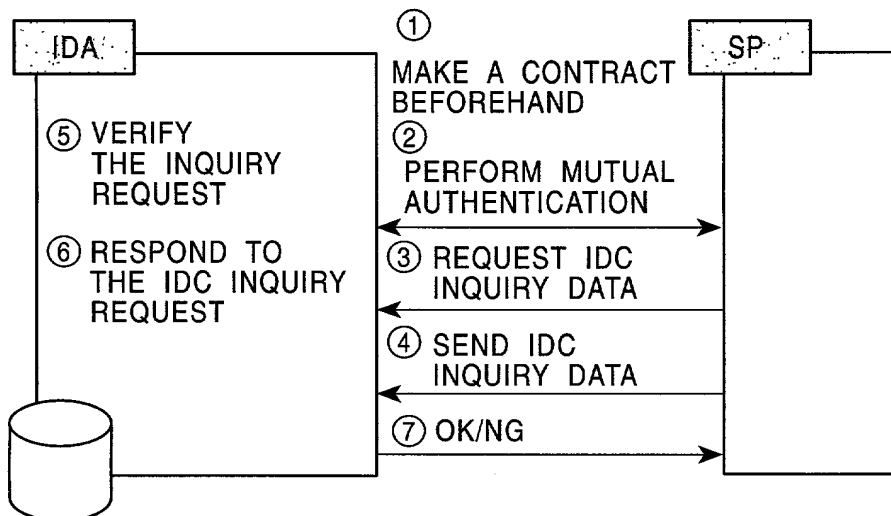
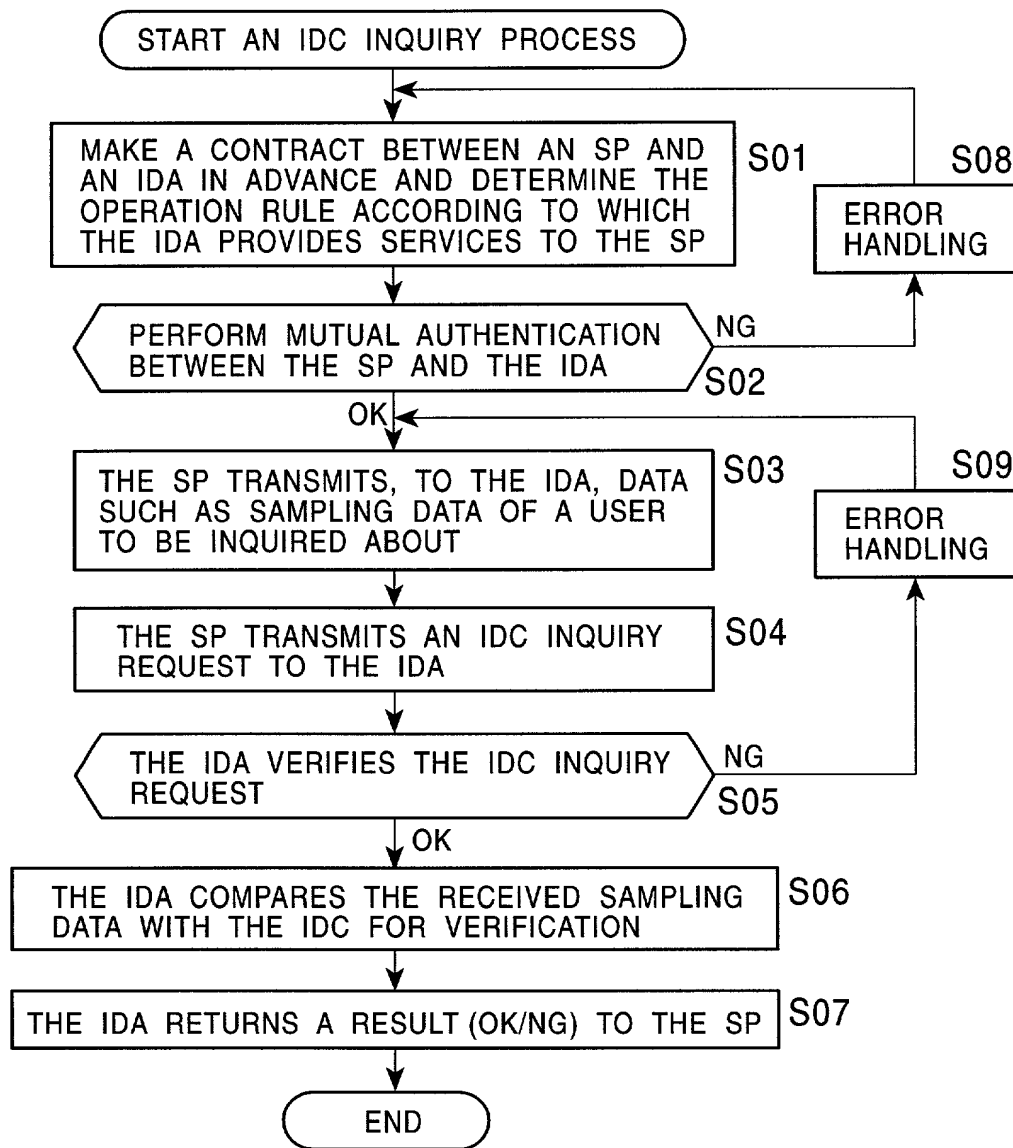


FIG. 19

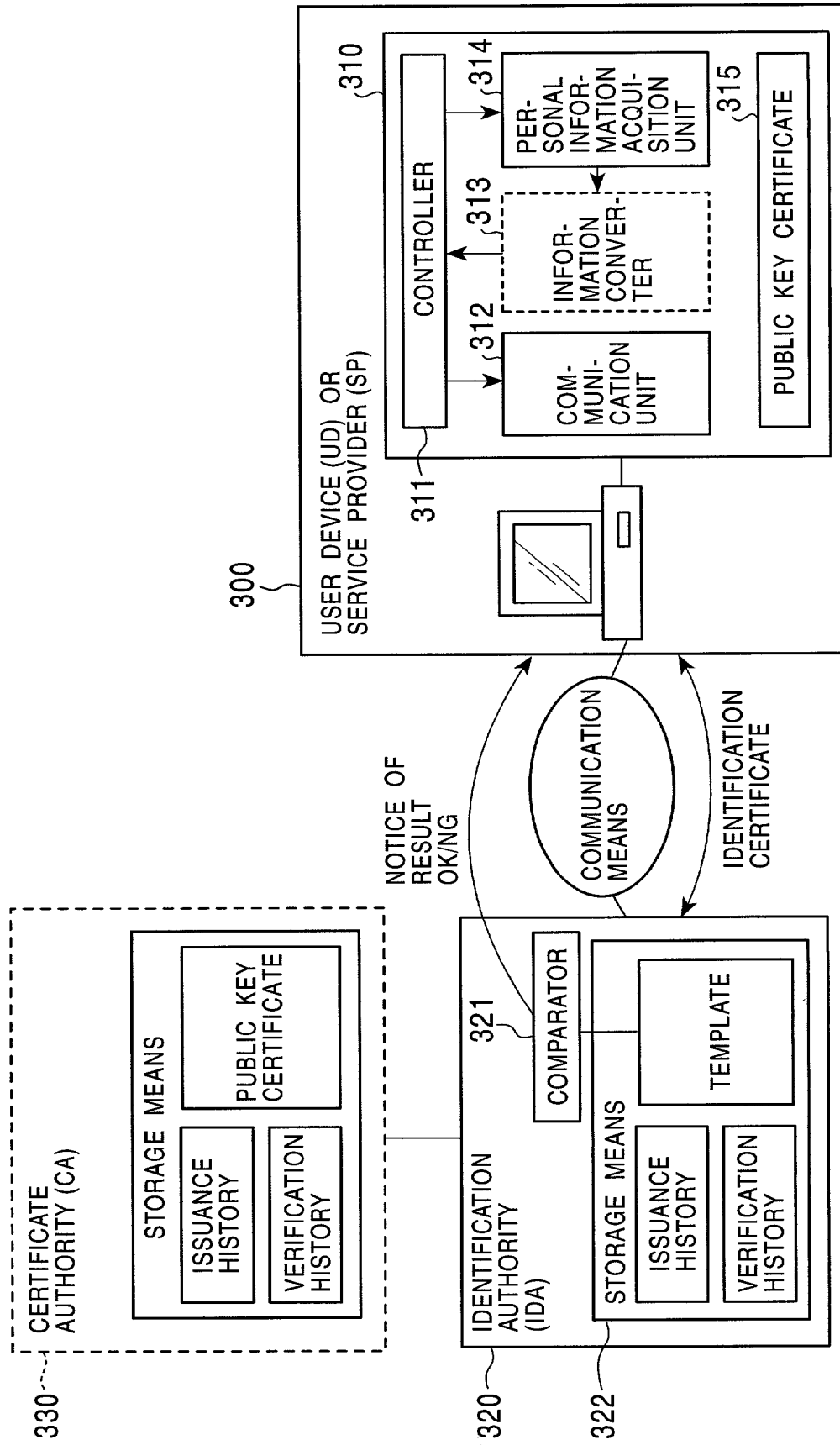


FIG. 20

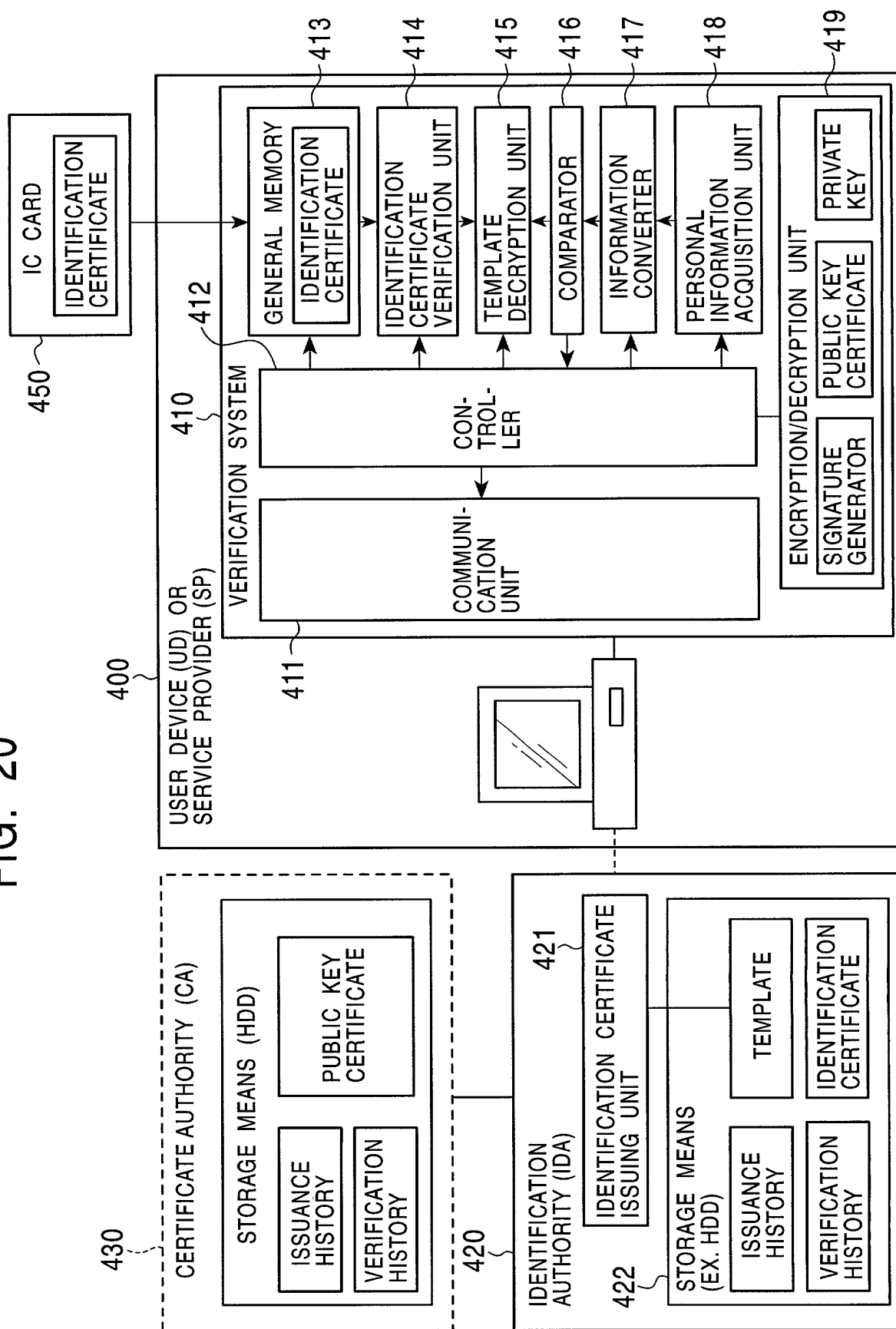


FIG. 21A

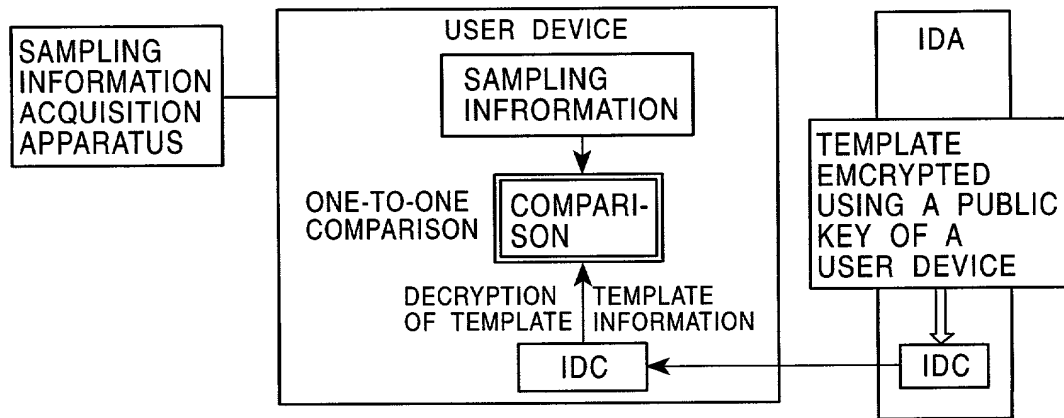


FIG. 21B

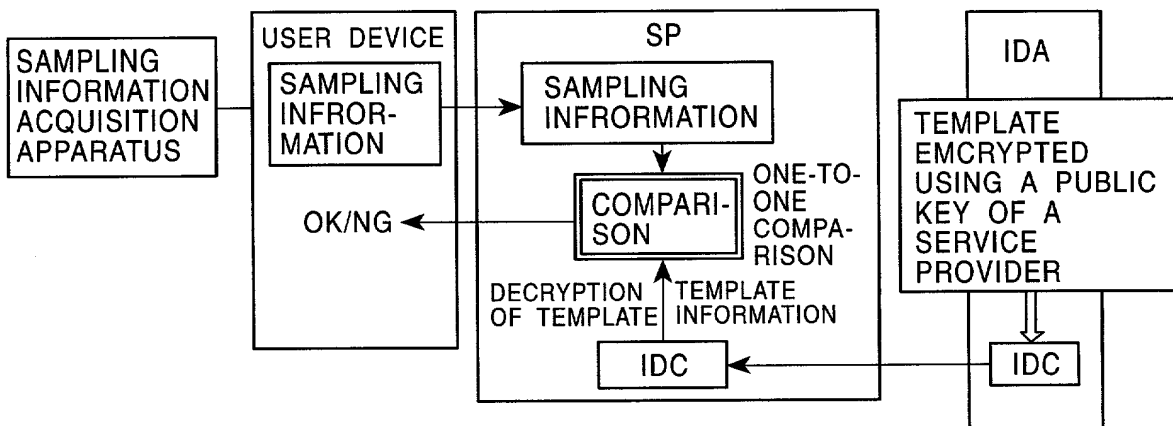


FIG. 21C

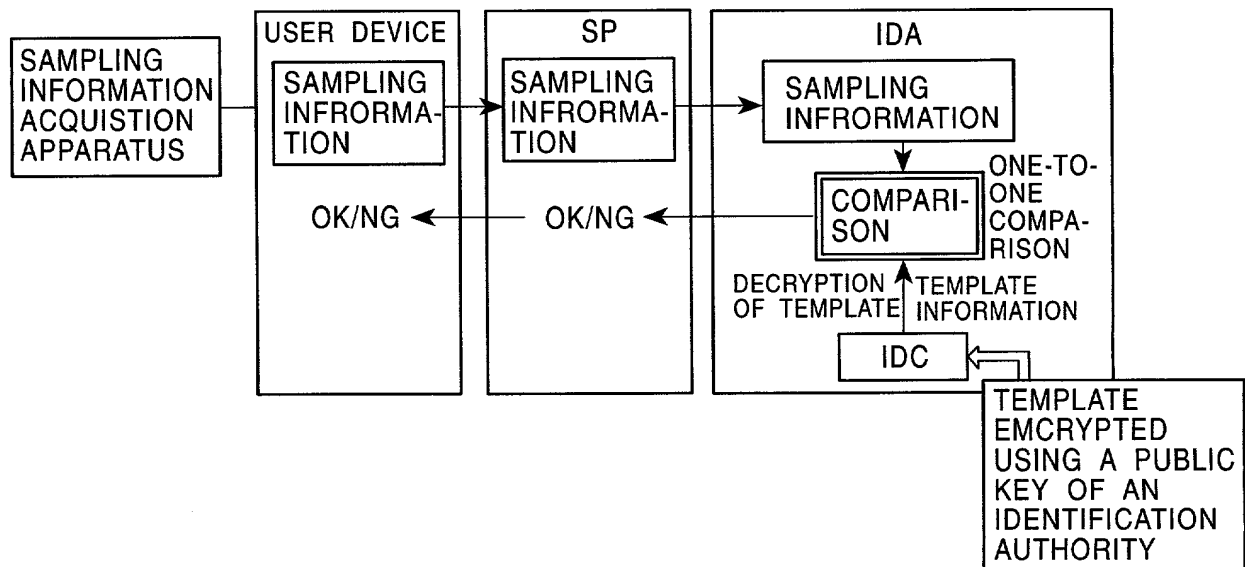


FIG. 22

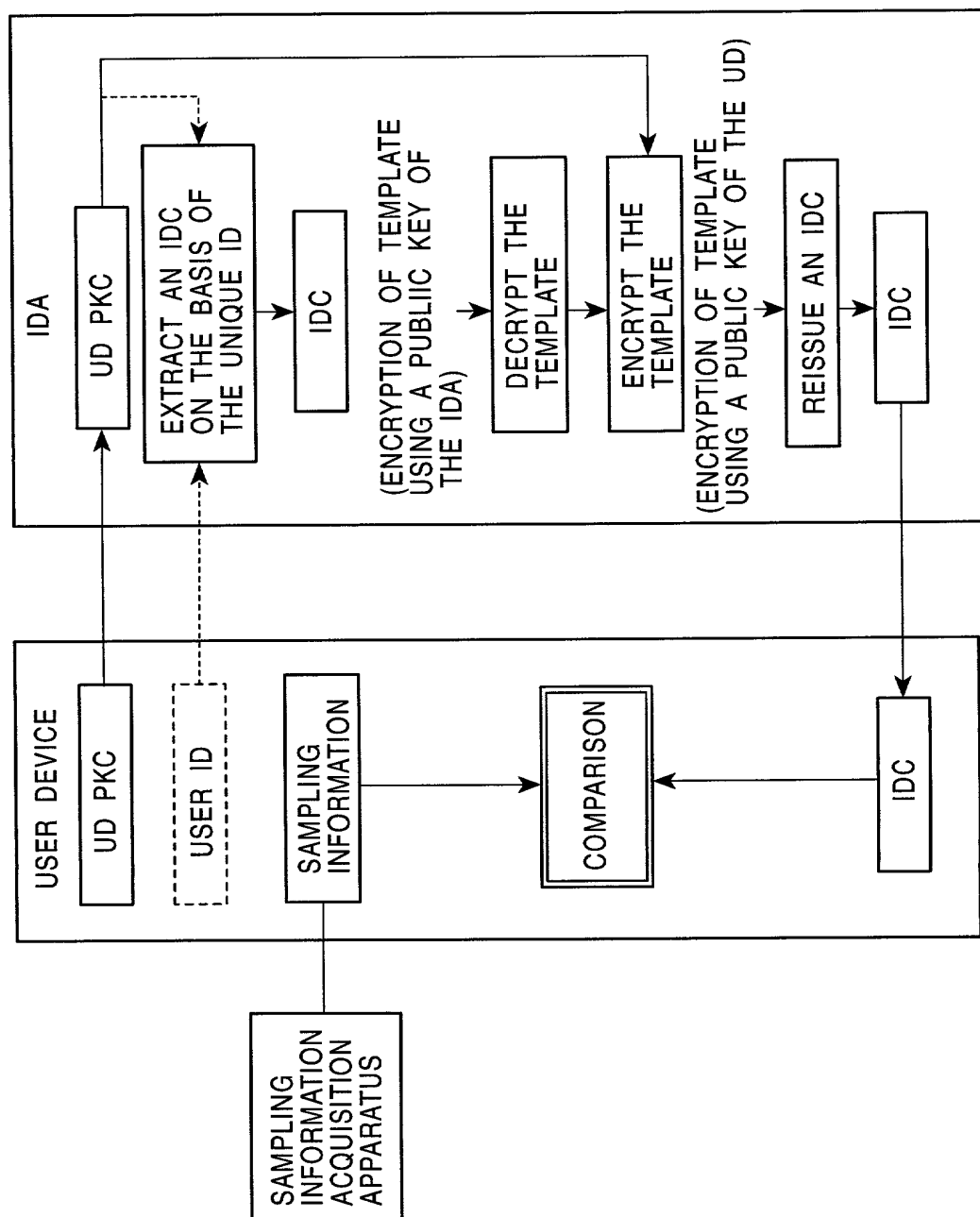


FIG. 23

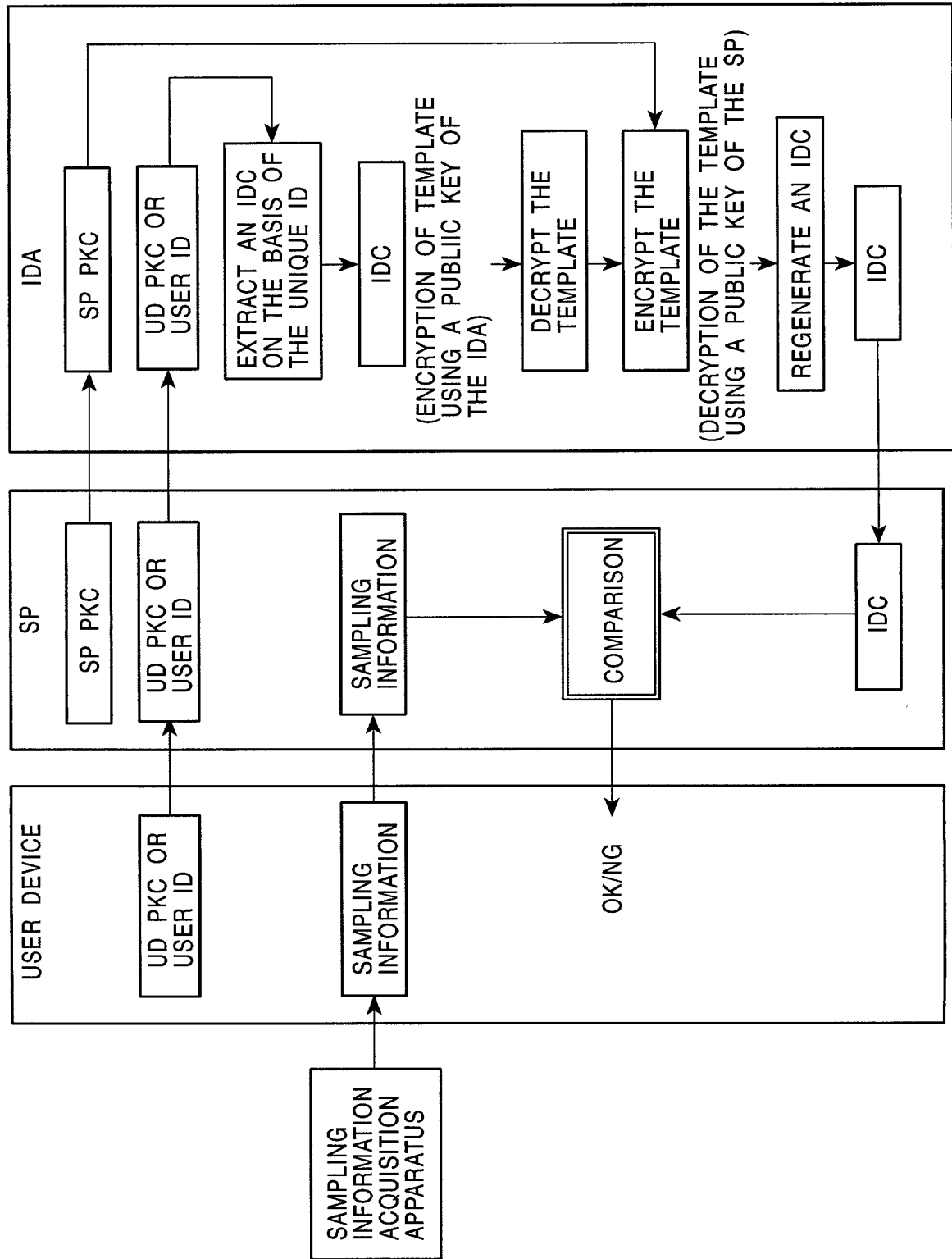


FIG. 24

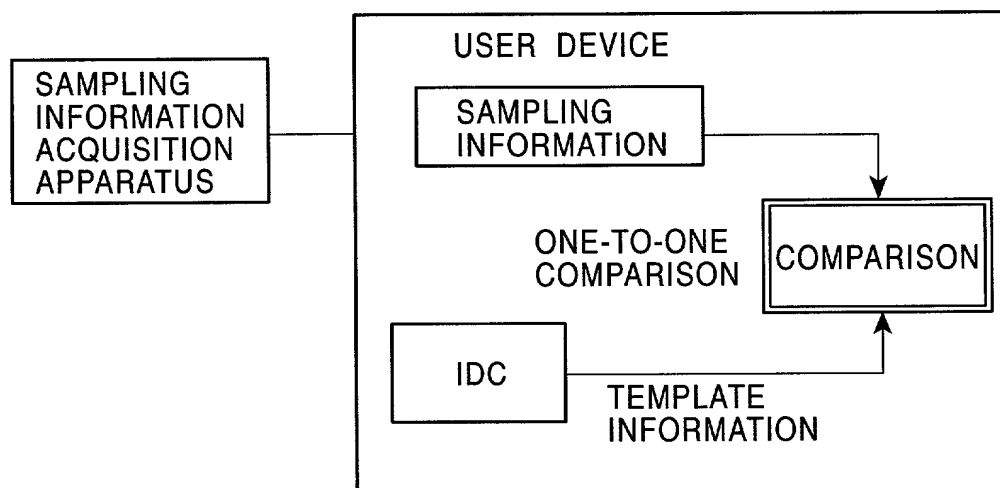




FIG. 25

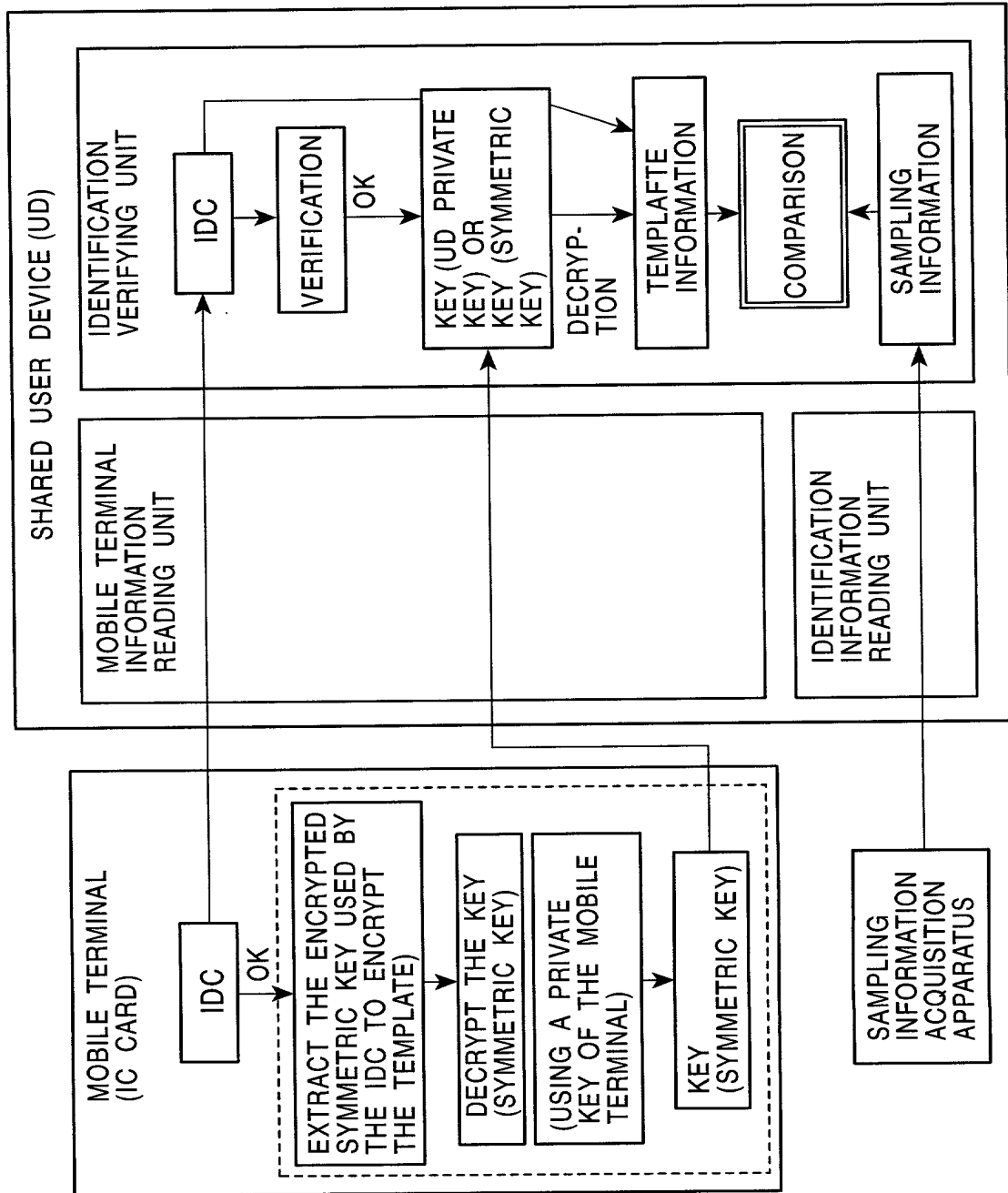


FIG. 26

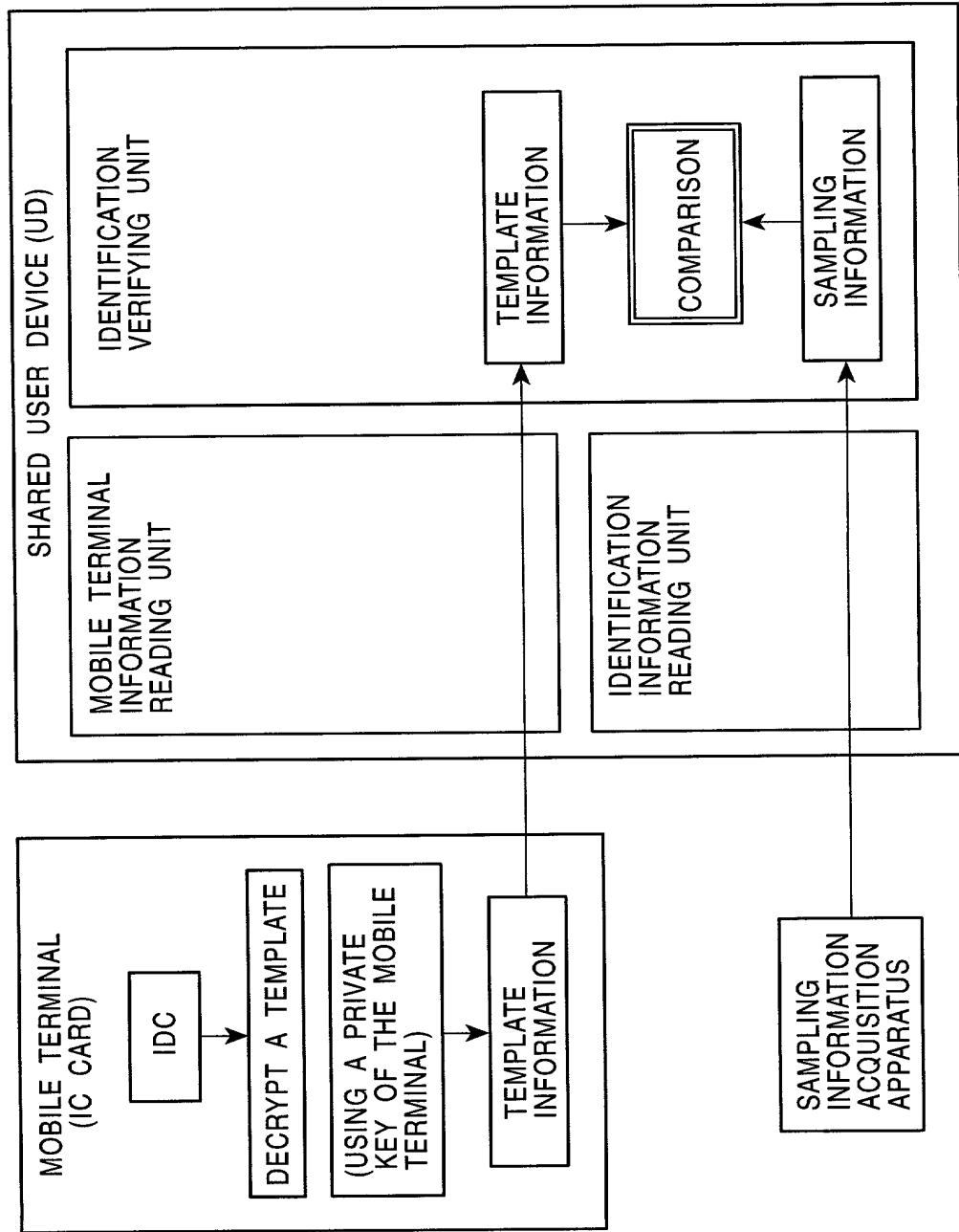


FIG. 27

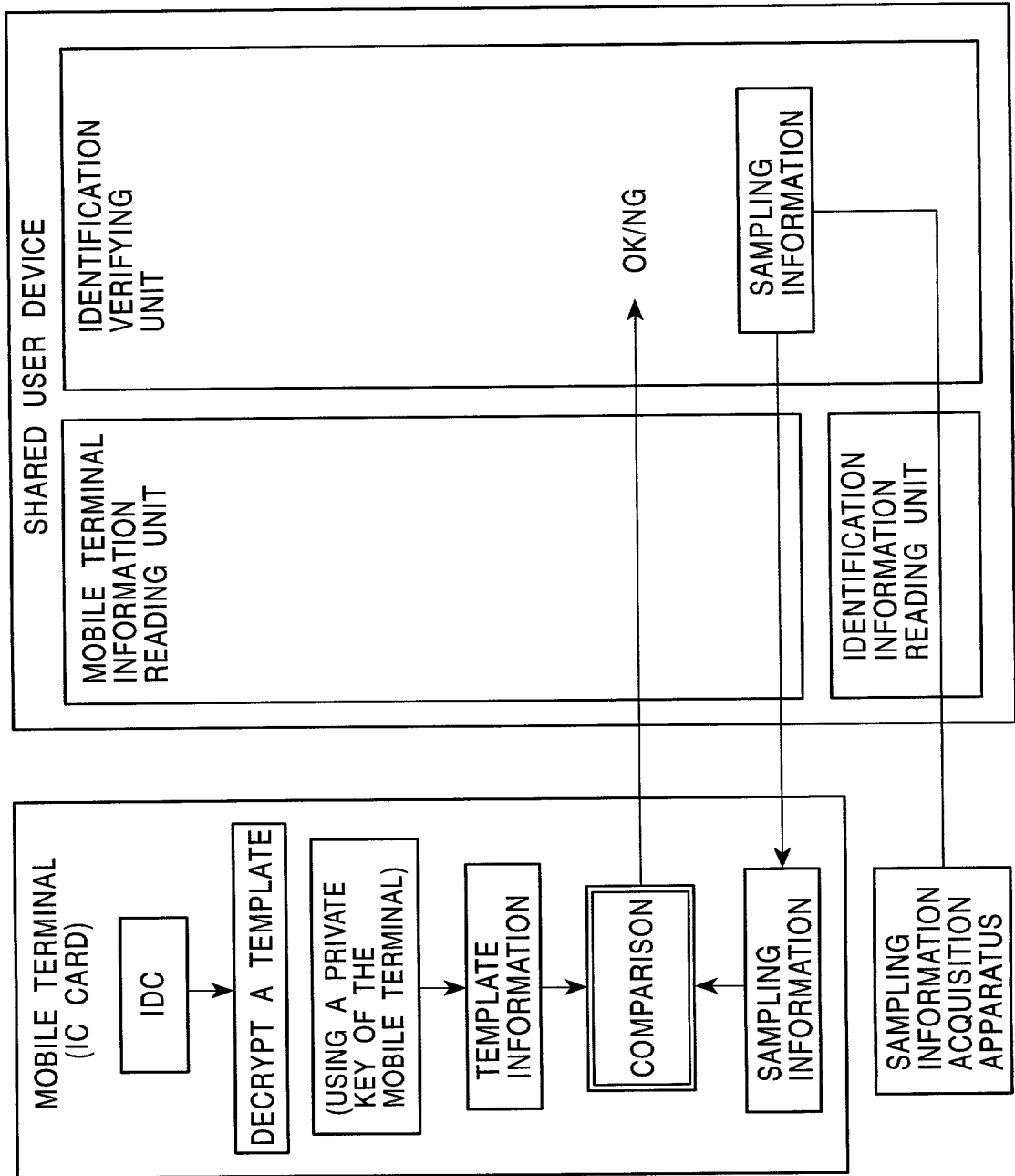


FIG. 28

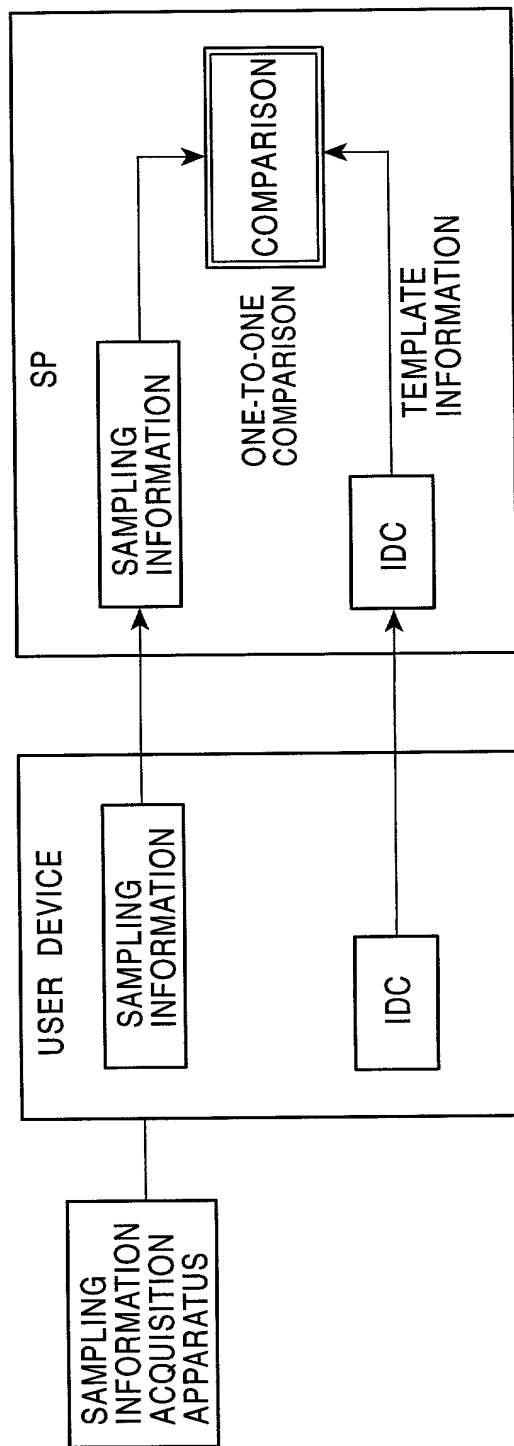


FIG. 29

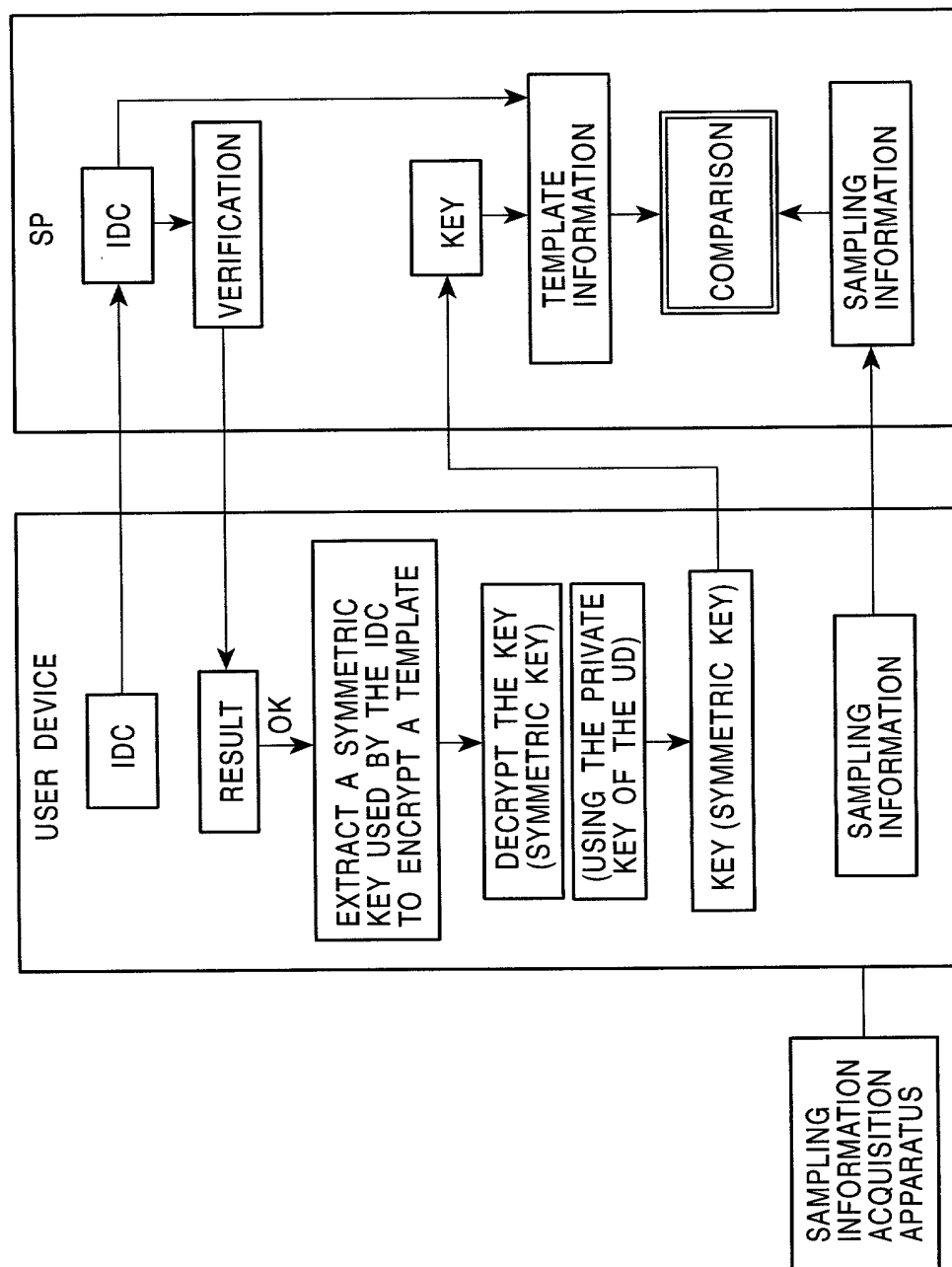


FIG. 30

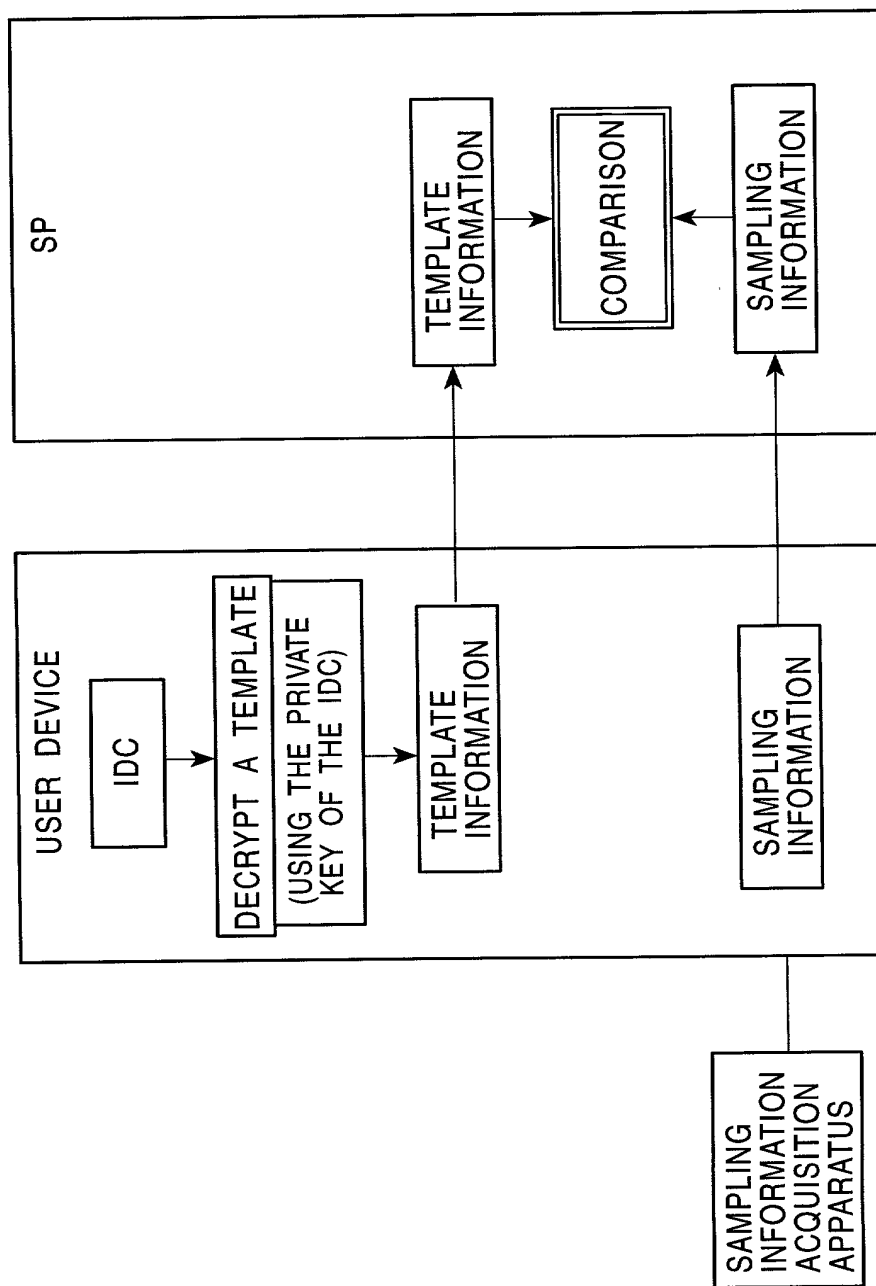


FIG. 31

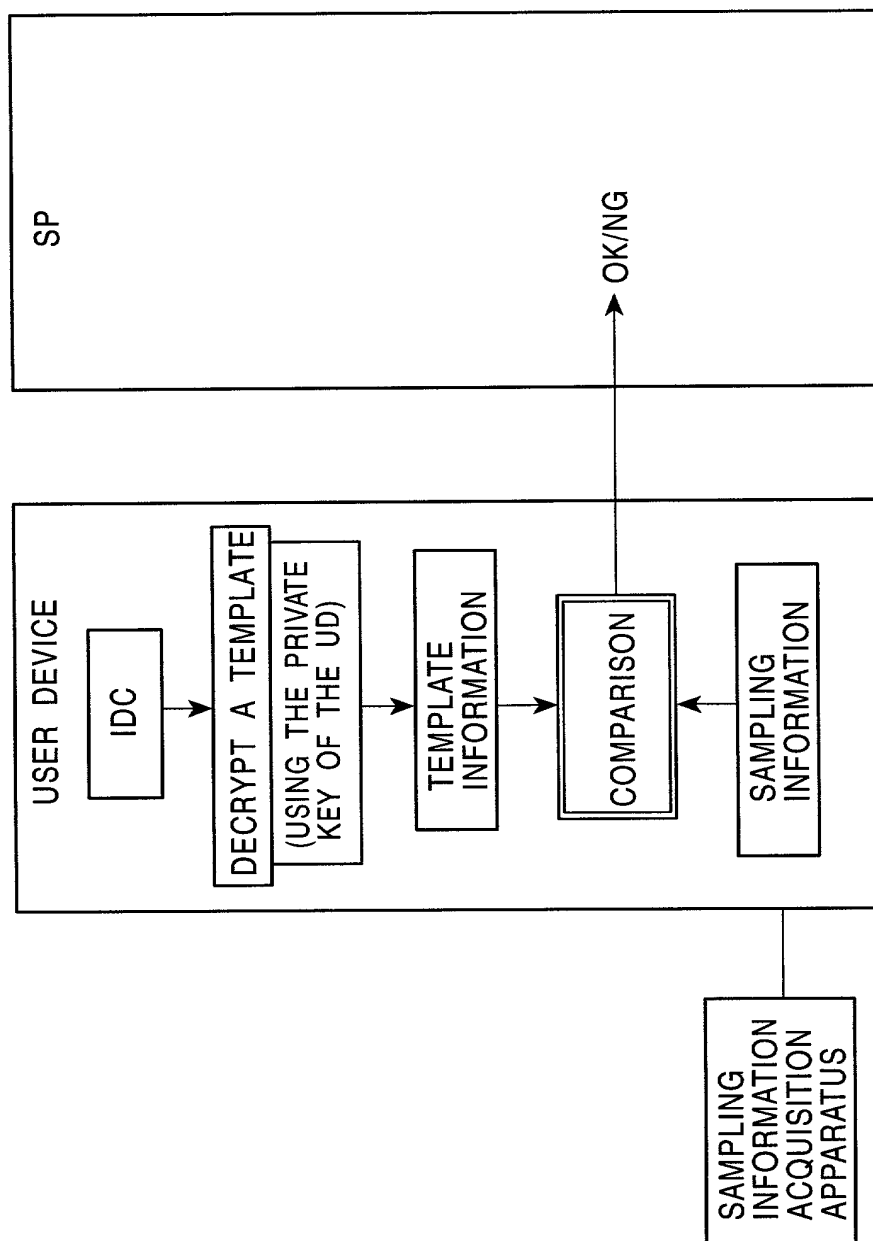


FIG. 32

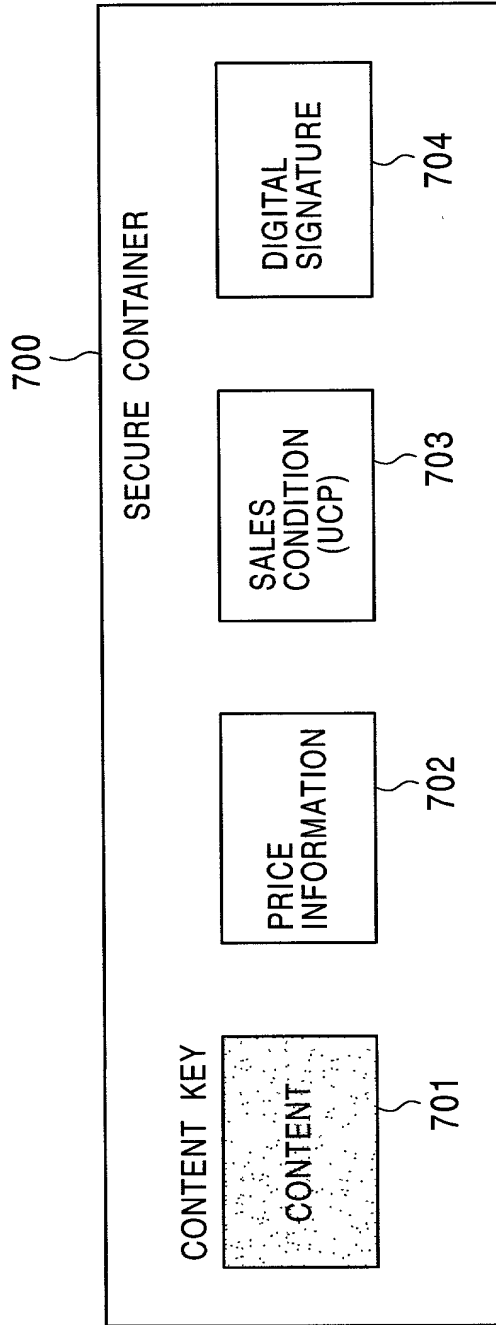




FIG. 33

USER ID	IDENTIFICATION CERTIFICATE (IDC) IDENTIFIER
ABC0001	CDE00021
ABC0002	CDE00027
ABC0003	CDE03211
⋮	⋮
BBC0231	EED02333

FIG. 34

DATA TYPE	
TYPE OF DEALING POLICY	
PERIOD DURING WHICH DEALING POLICY IS VALID	
CONTENT ID	
CONTENT PROVIDER ID	
DEALING POLICY ID	
VERSION OF THE DEALING POLICY	
AREA CODE	
USABLE DEVICE CONDITIONS	
USERS PERMITTED TO USE THE CONTENT	
IDC IDENTIFIER LIST	
SERVICE PROVIDER ID	
UCP GENERATION MANAGEMENT INFORMATION	
MAXIMUM ALLOWABLE NUMBER OF SECONDARY DISTRIBUTIONS	
NUMBER OF RULES	
RULE ADDRESS	
RULE 1	RULE NUMBER
	TYPE OF PERMITTED USAGE
	⋮
⋮	⋮
RULE N	RULE NUMBER
	TYPE OF PERMITTED USAGE
	⋮
(INDICATION OF WHETHER THE SIGNATURE HAS BEEN VERIFIED)	
PUBLIC KEY CERTIFICATE	
SIGNATURE	

711

712

713

FIG. 35

RULE NUMBER	PERMITTED USAGE	PERIOD	NUMBER OF TIMES CONTENT IS USED	COPY
1	PLAYBACK	NOT LIMITED	NOT LIMITED	—
2		LIMITED	NOT LIMITED	—
3		NOT LIMITED	LIMITED	—
4	COPY	NOT LIMITED	NOT LIMITED	NOT LIMITED
5		LIMITED	NOT LIMITED	NOT LIMITED
6		NOT LIMITED	LIMITED	NOT LIMITED
7		NOT LIMITED	NOT LIMITED	SCMS
8		LIMITED	NOT LIMITED	
9		NOT LIMITED	LIMITED	
10		NOT LIMITED	NOT LIMITED	OTHERS
11		LIMITED	NOT LIMITED	
12		NOT LIMITED	LIMITED	
13	CHANGING OF PERMITTED USAGE			
14	REDISTRIBUTION			
15	UPGRADE TO AN ALBUM			
16	PERMISSION OF TRANSFERRING MANAGEMENT			

FIG. 36

721

FIG. 37

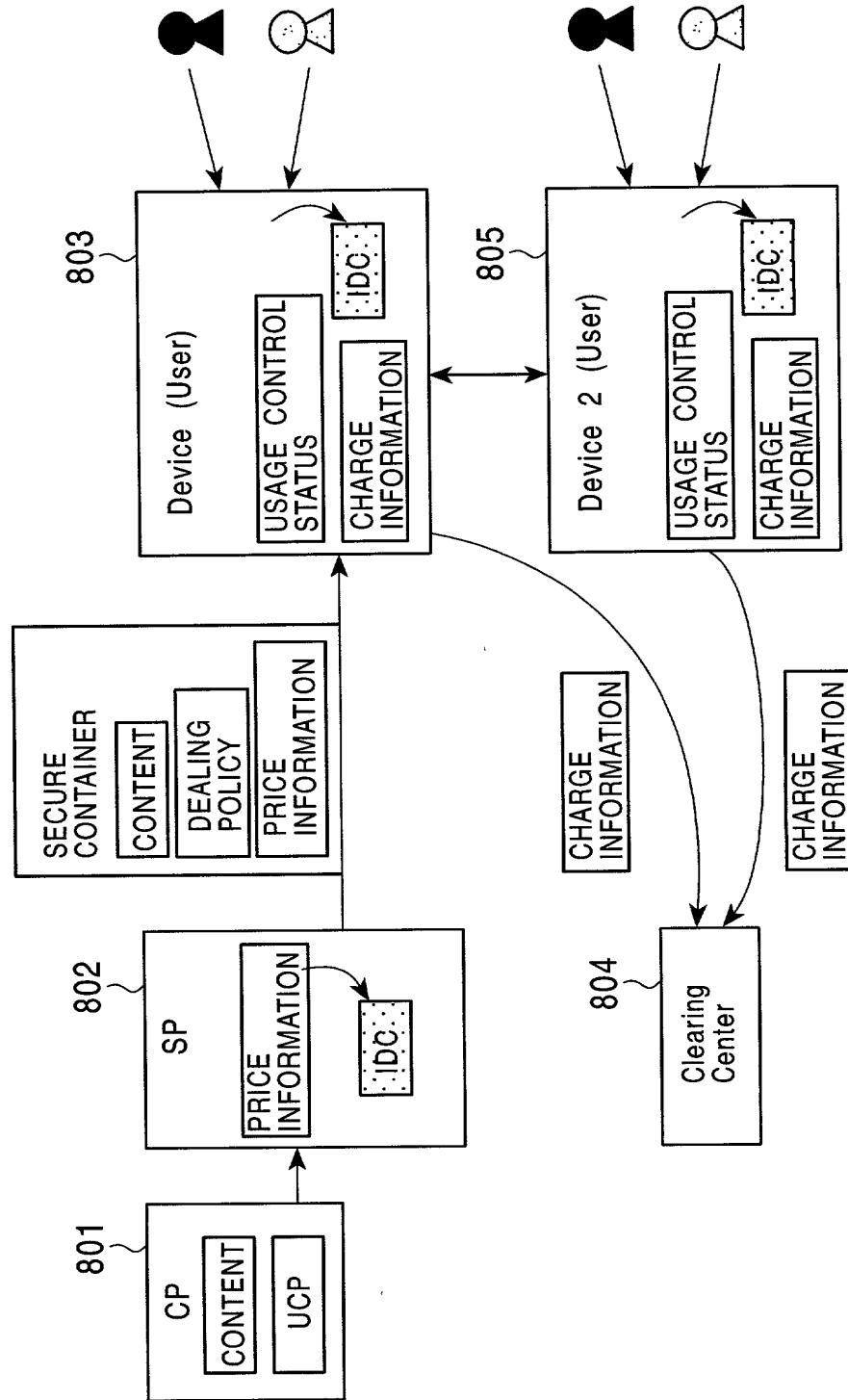




FIG. 39

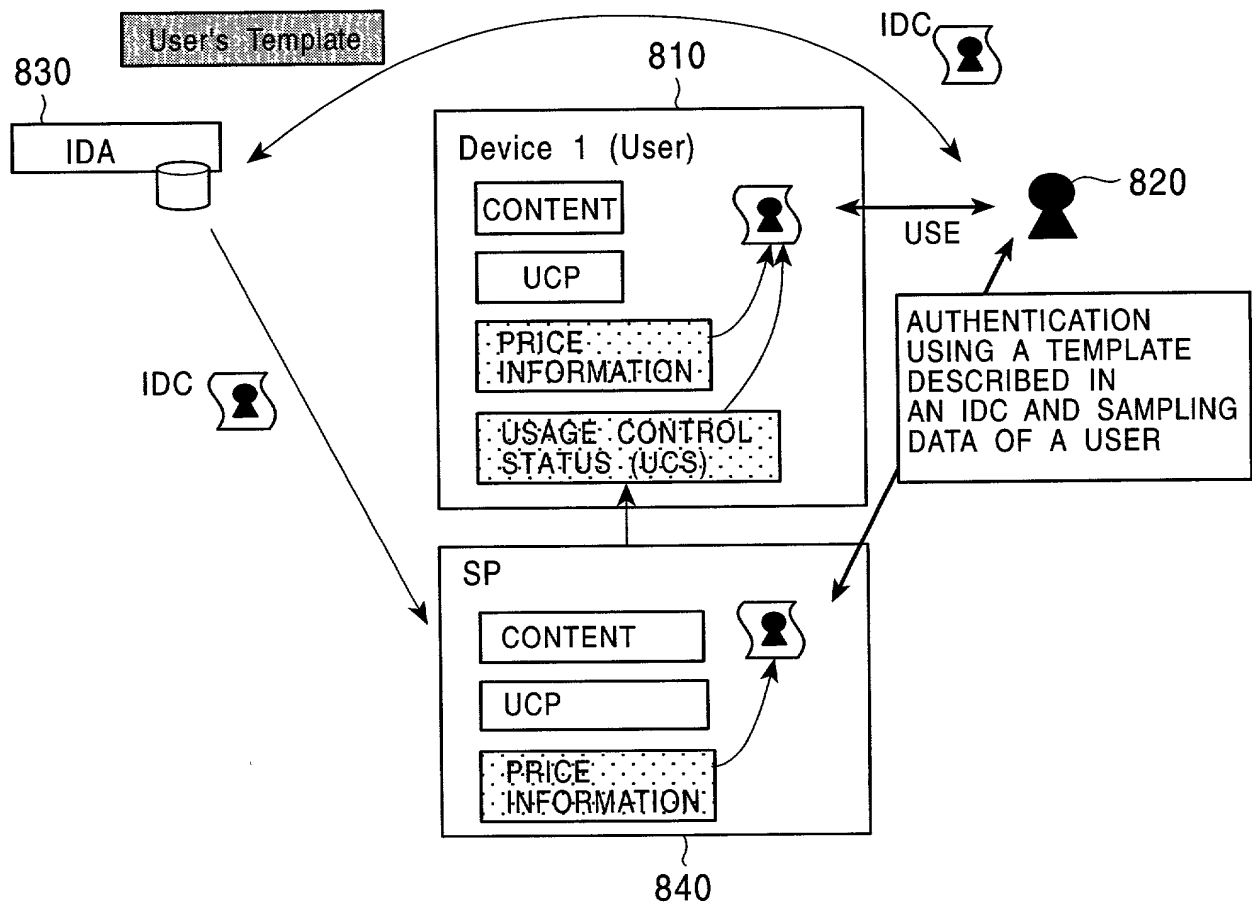


FIG. 40

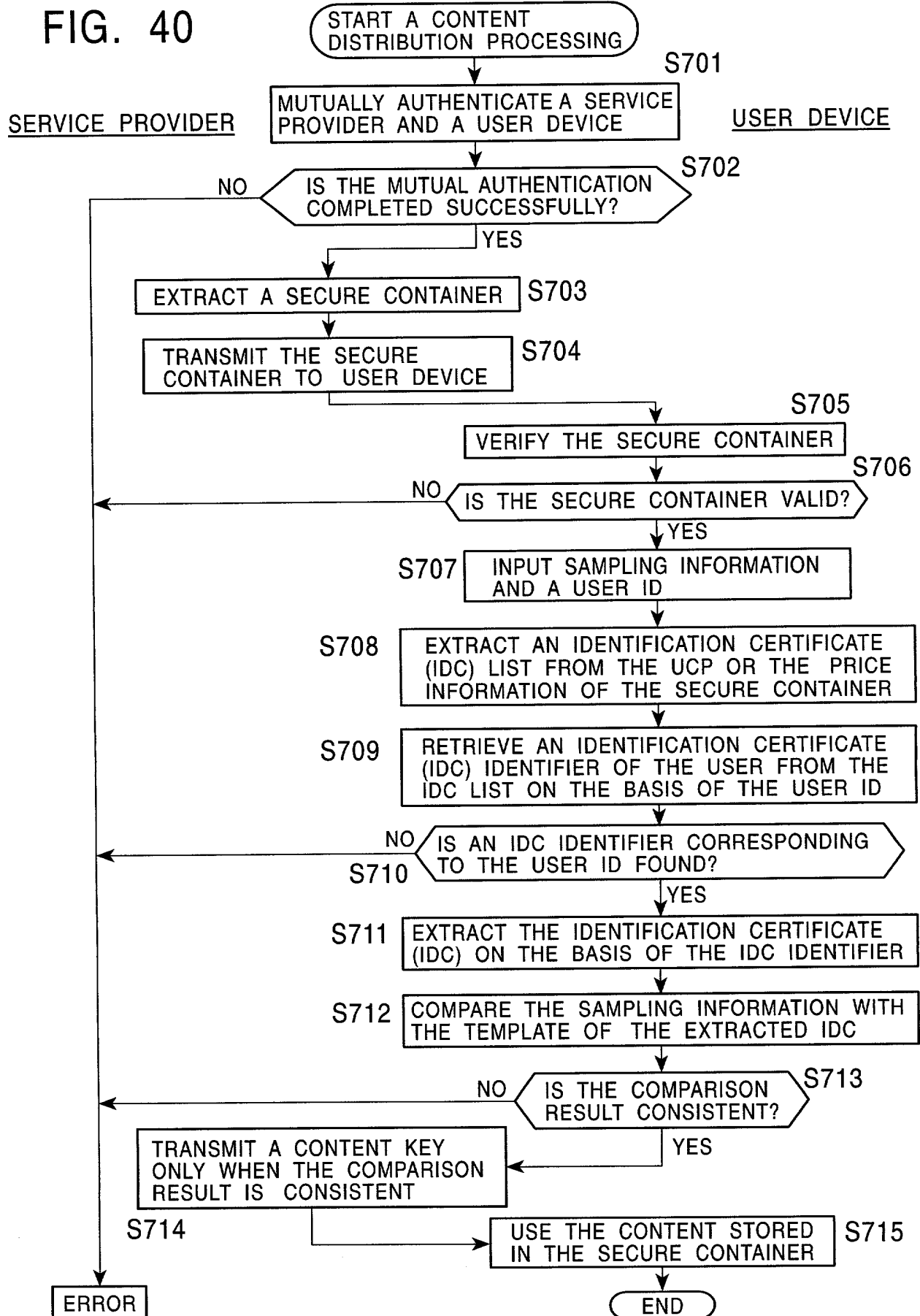




FIG. 41

SERVICE PROVIDER

USER DEVICE

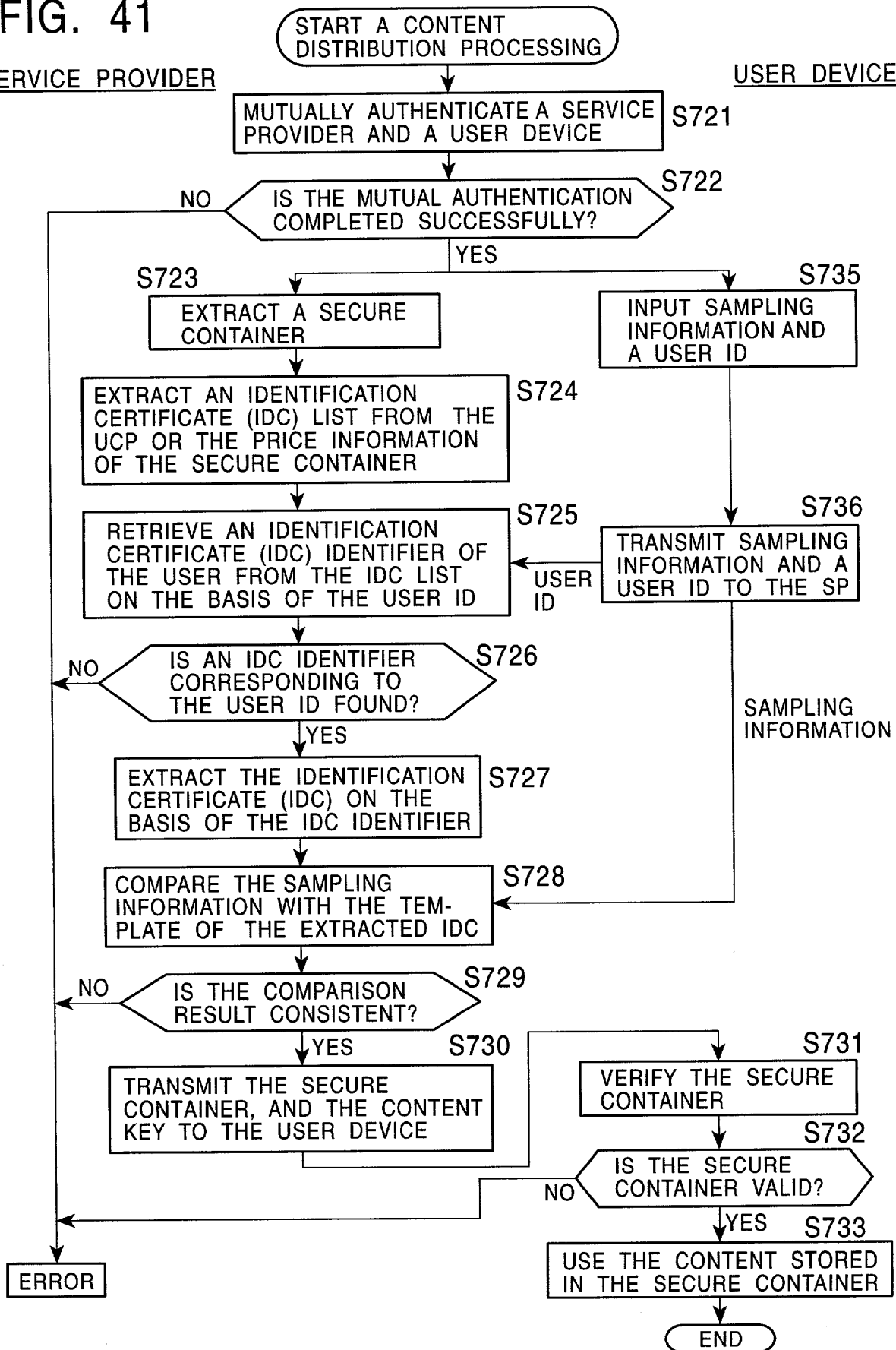


FIG. 42

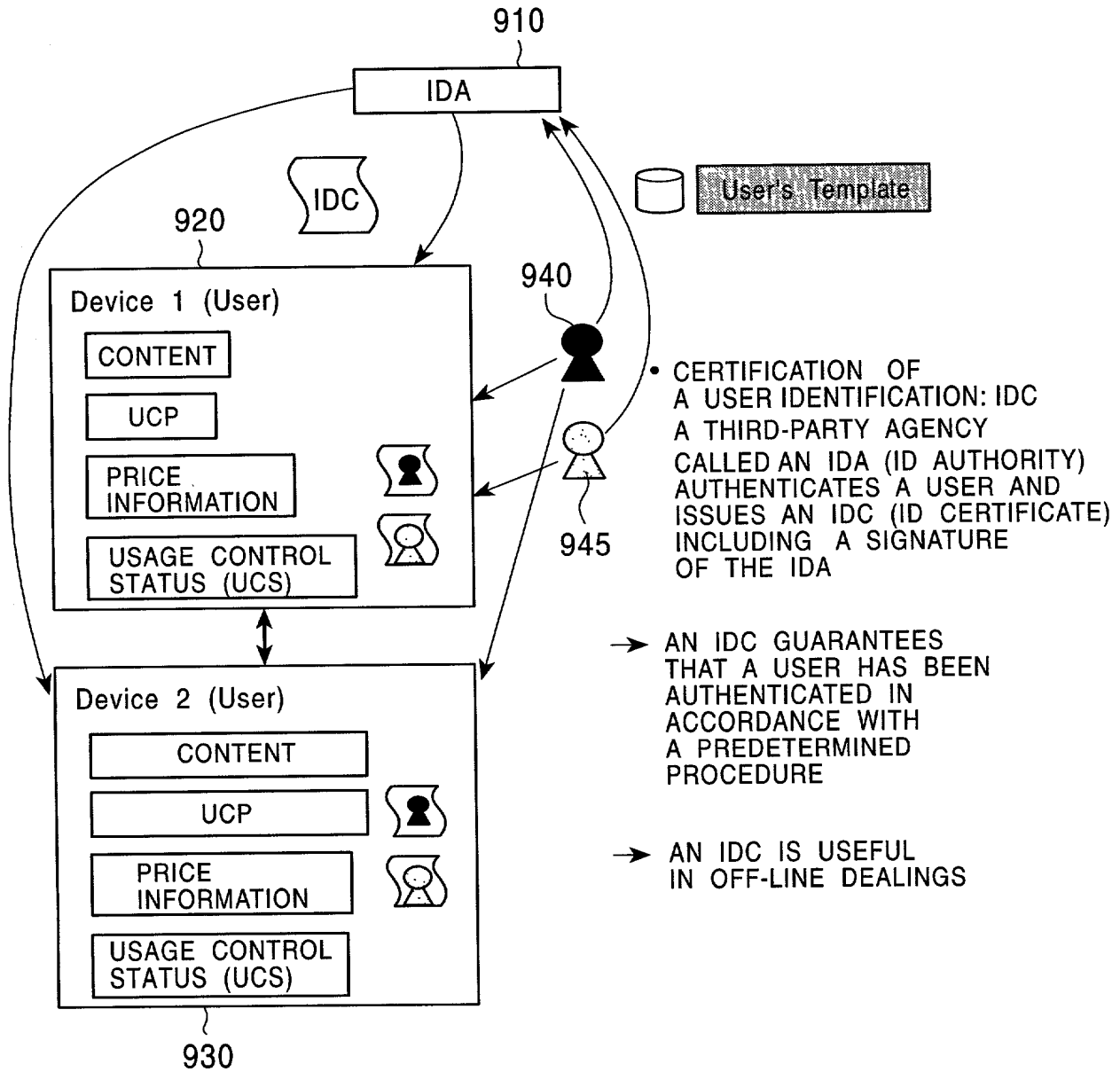


FIG. 43

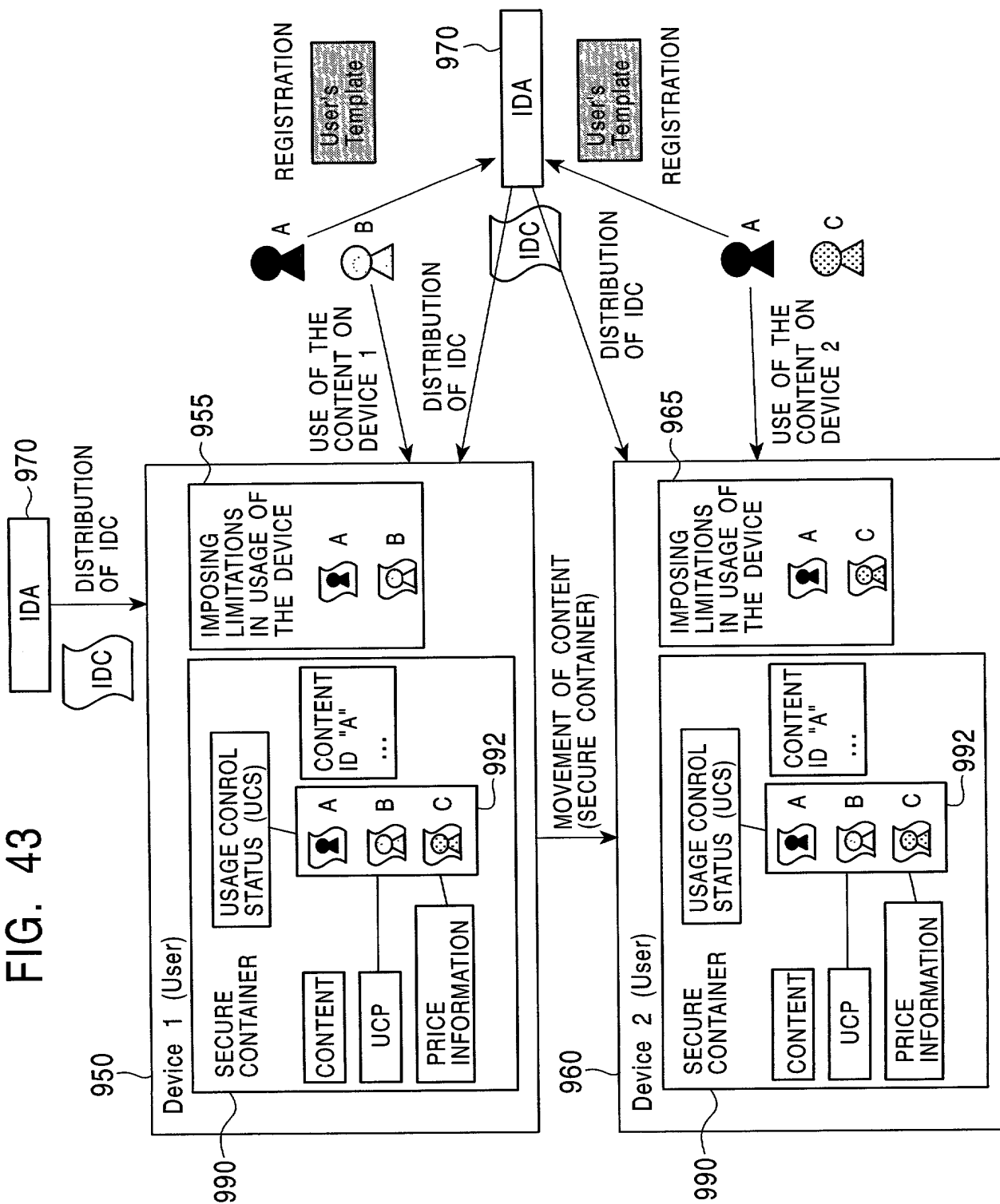


FIG. 44

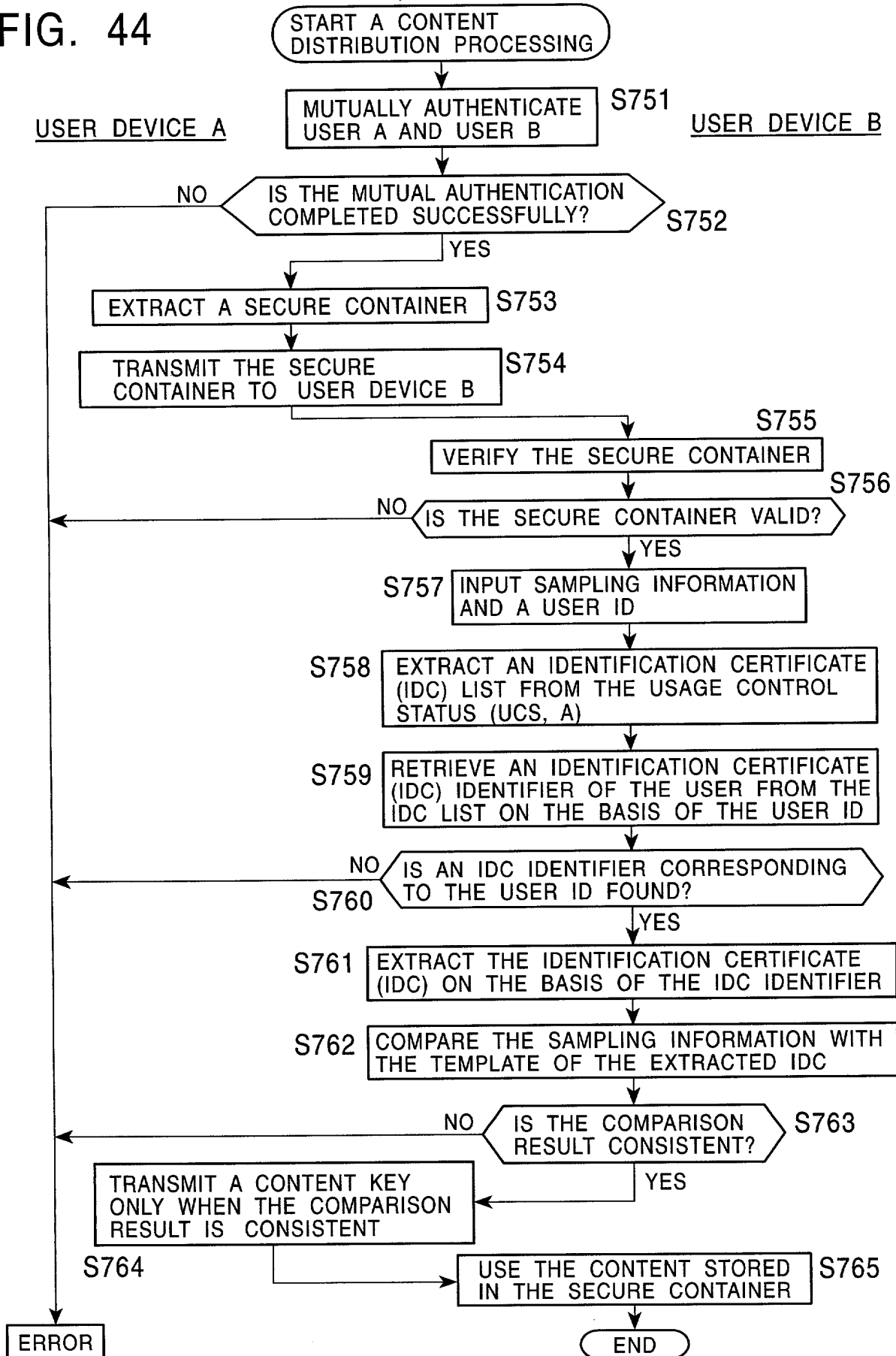


FIG. 45

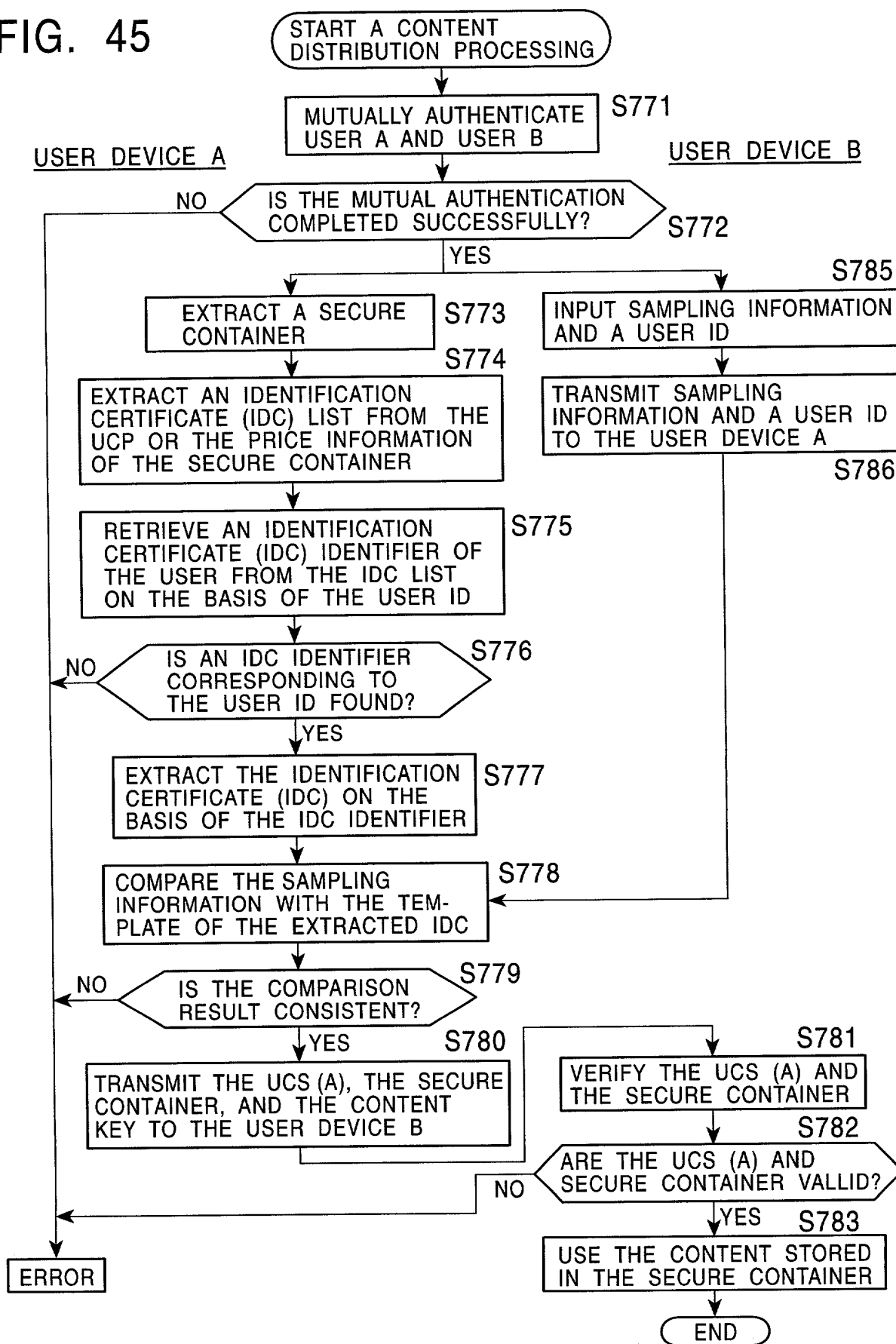


FIG. 46

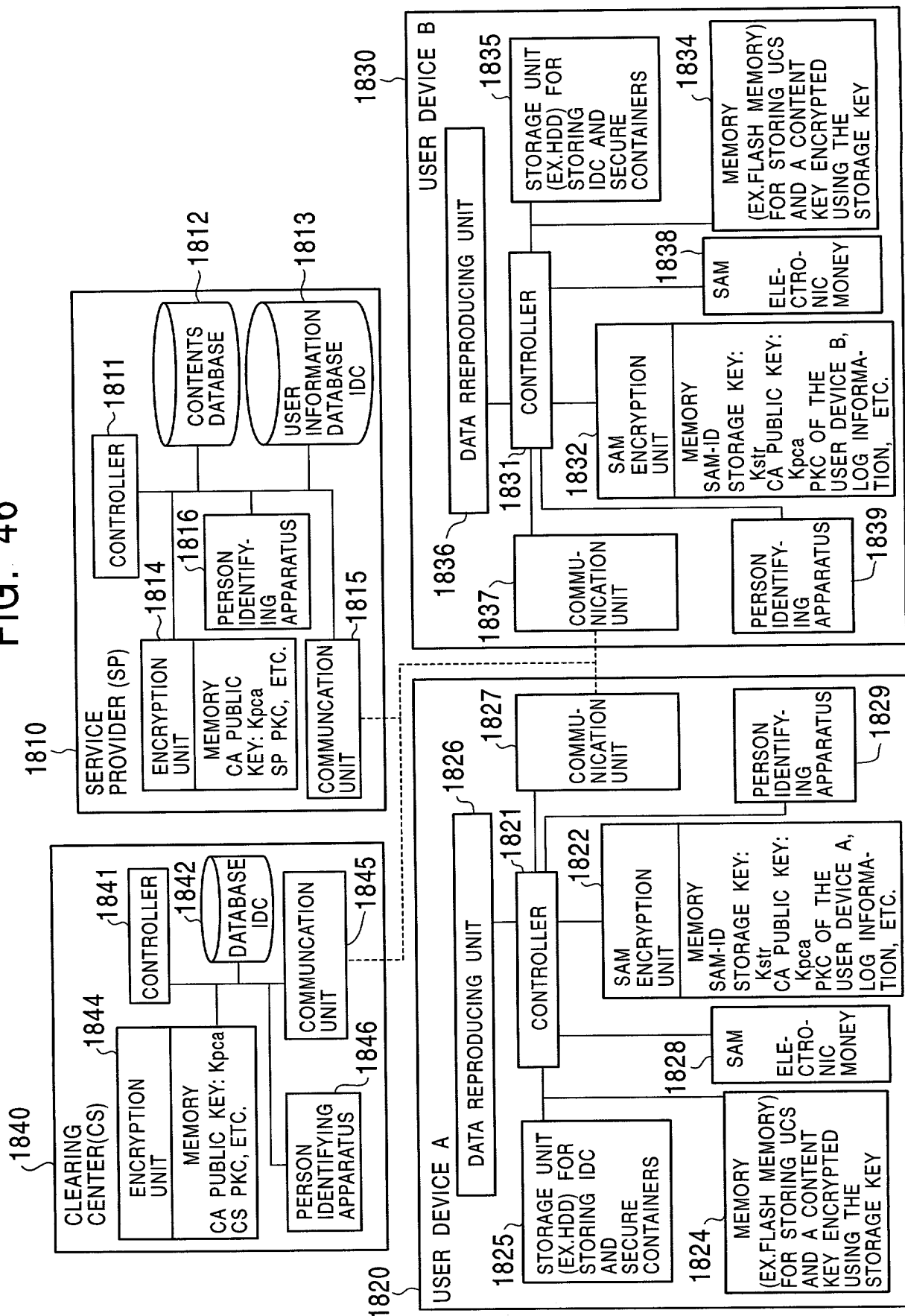


FIG. 47A

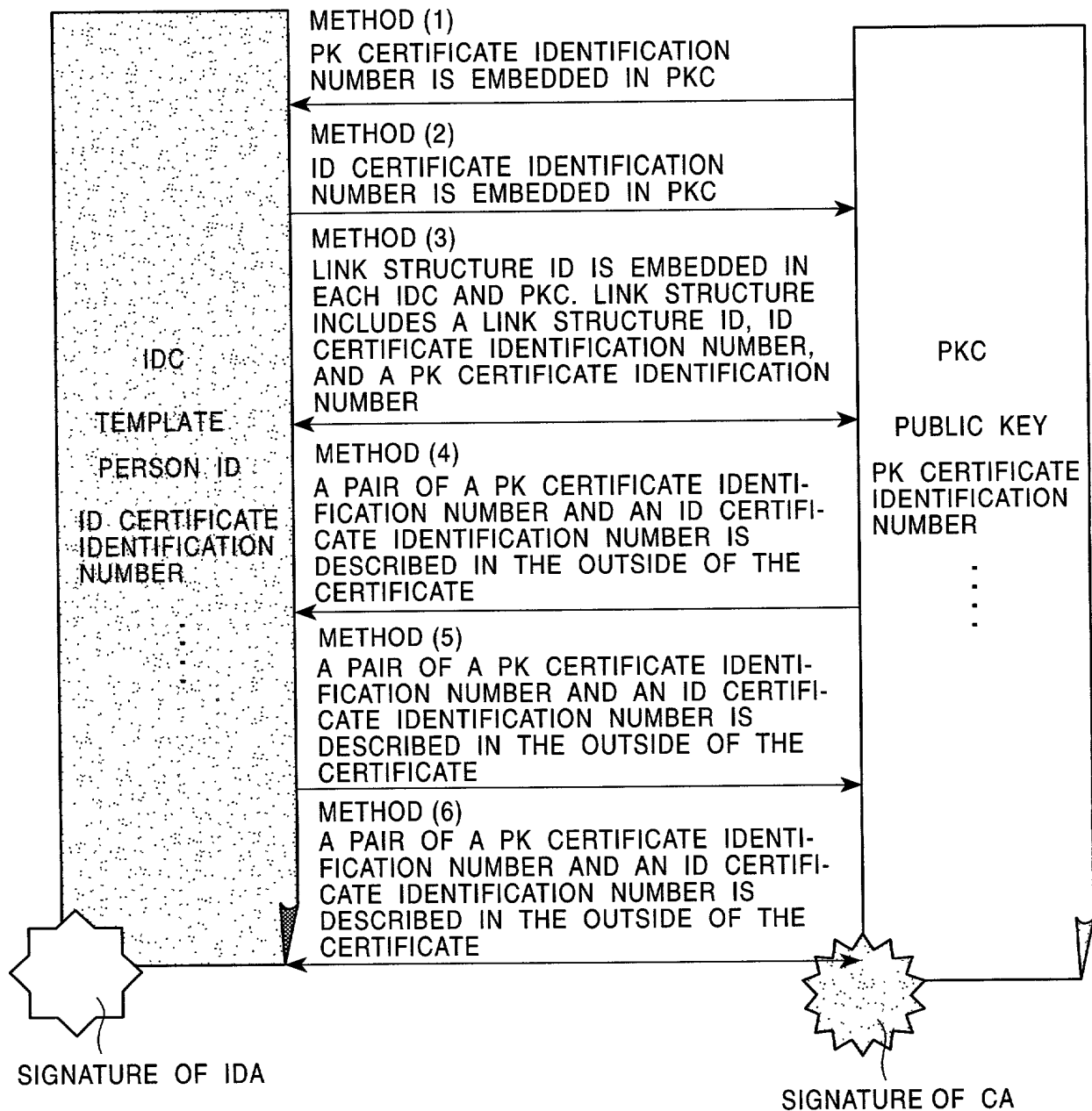


FIG. 47B

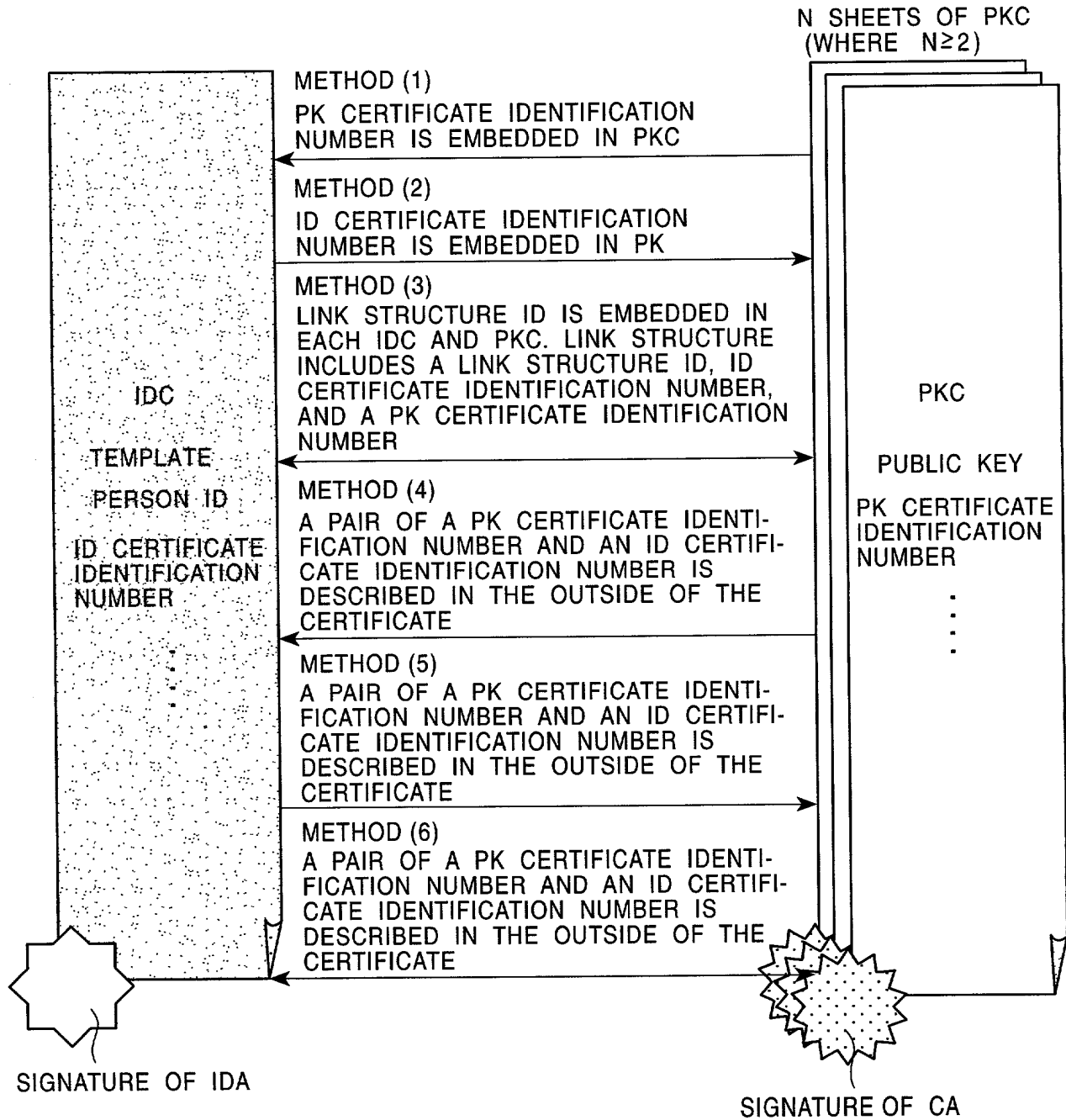




FIG. 48A

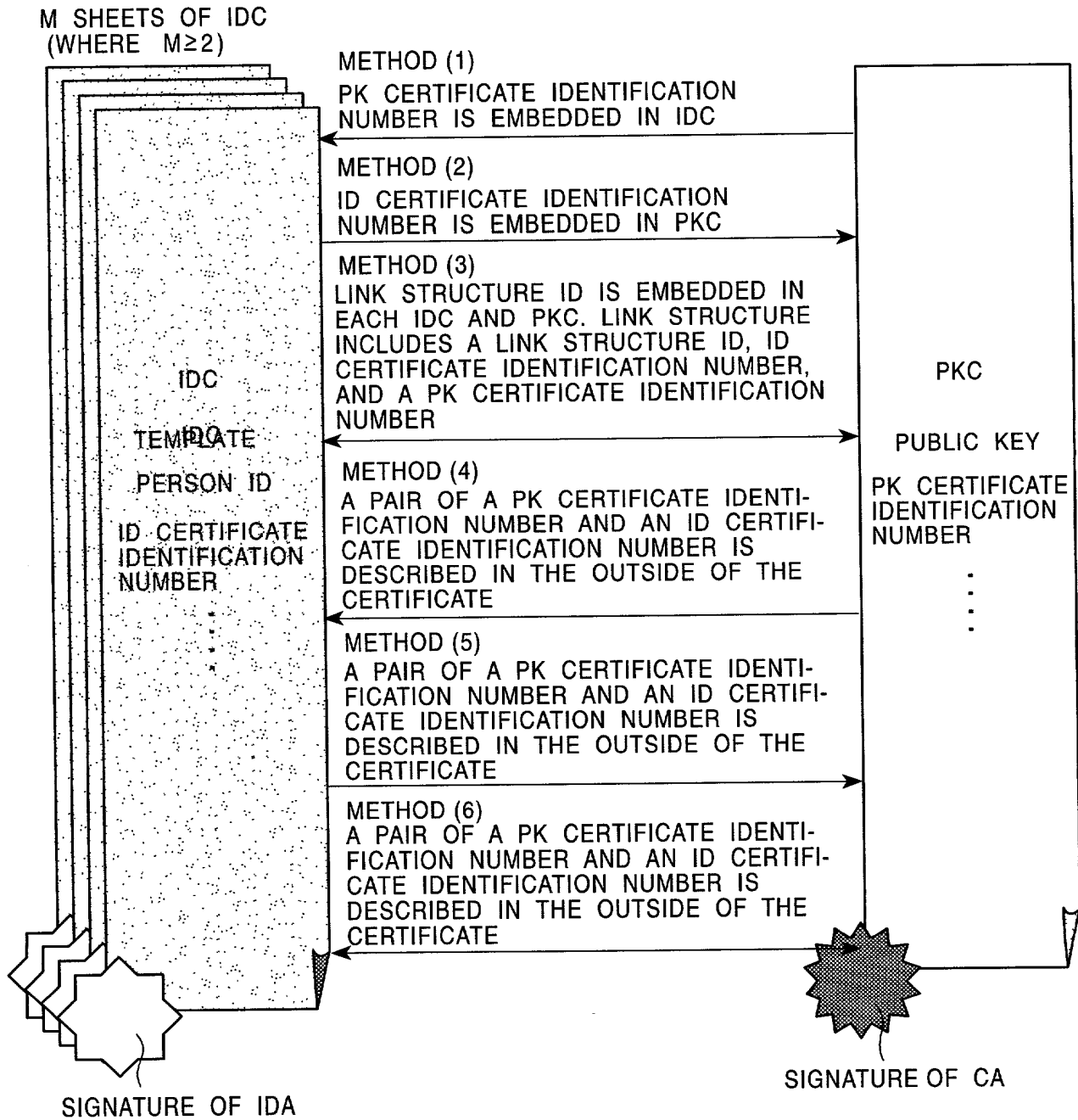


FIG. 48B

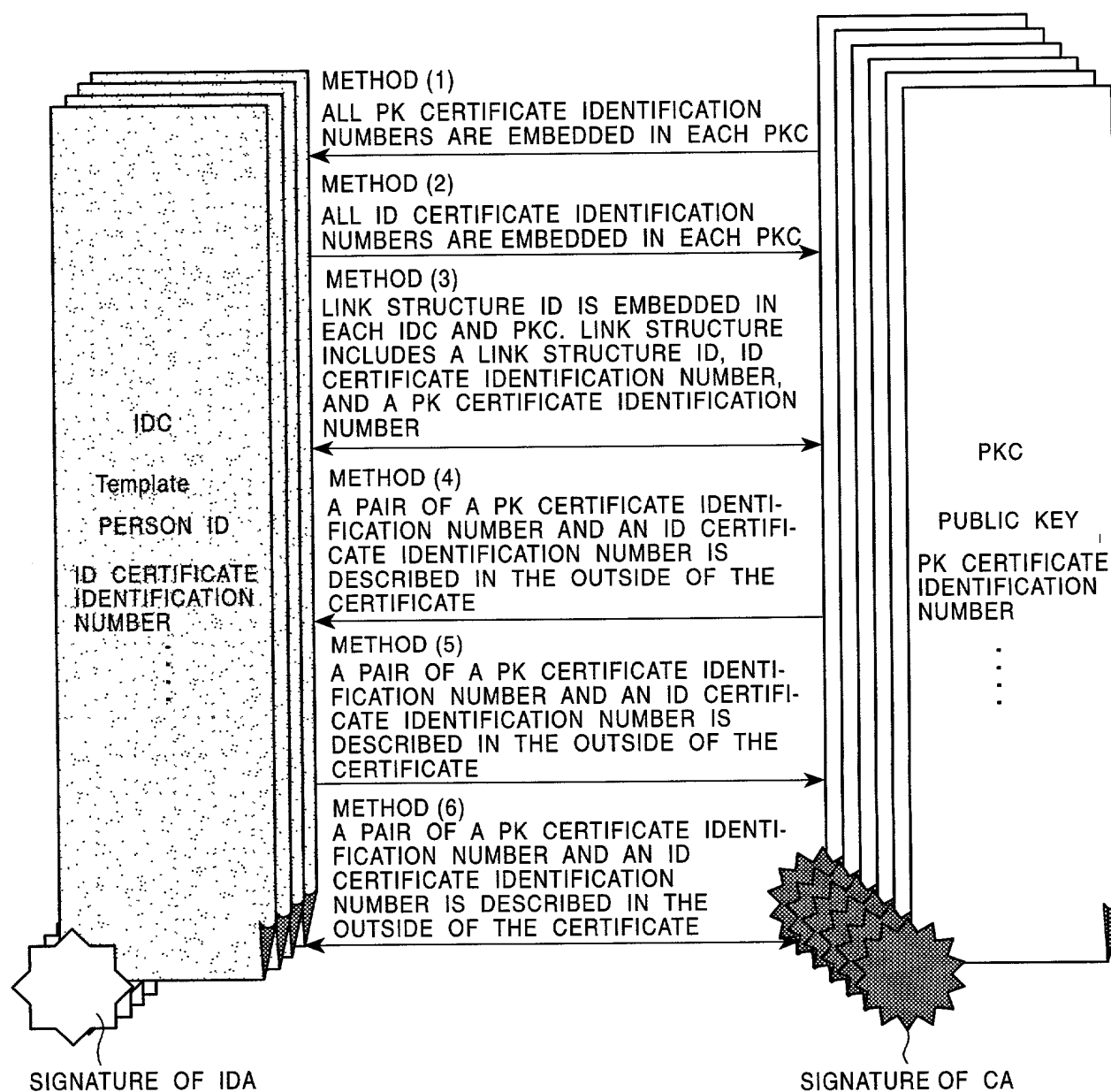


FIG. 49A

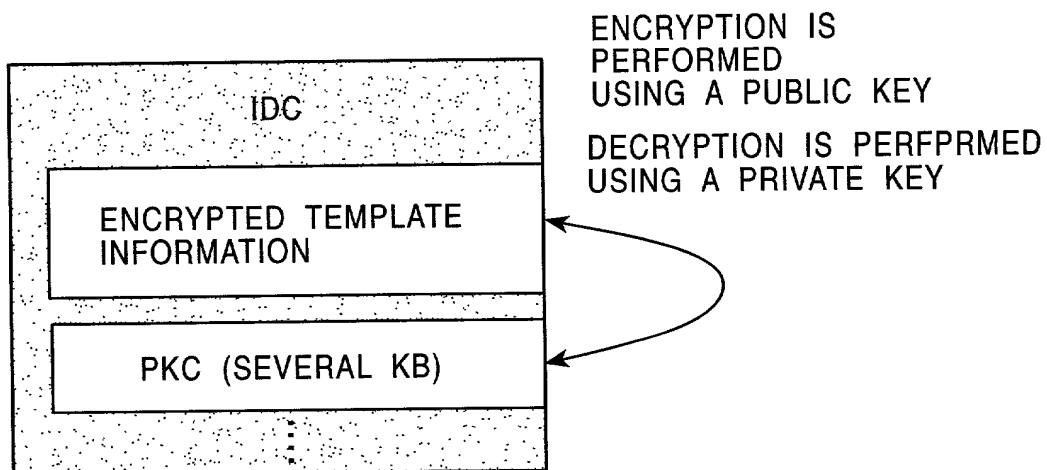


FIG. 49B

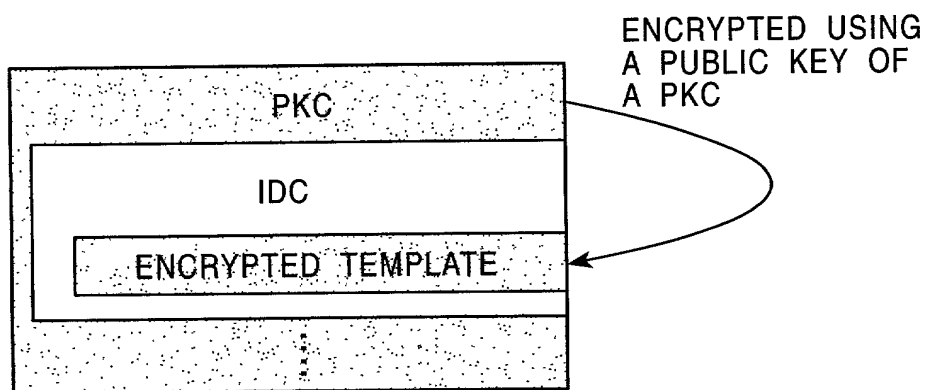


FIG. 50A

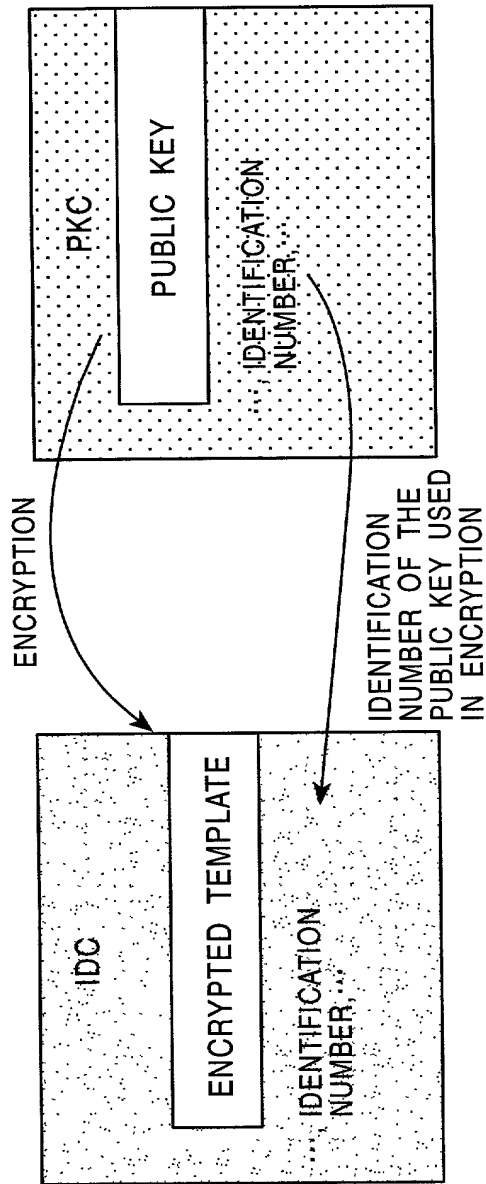
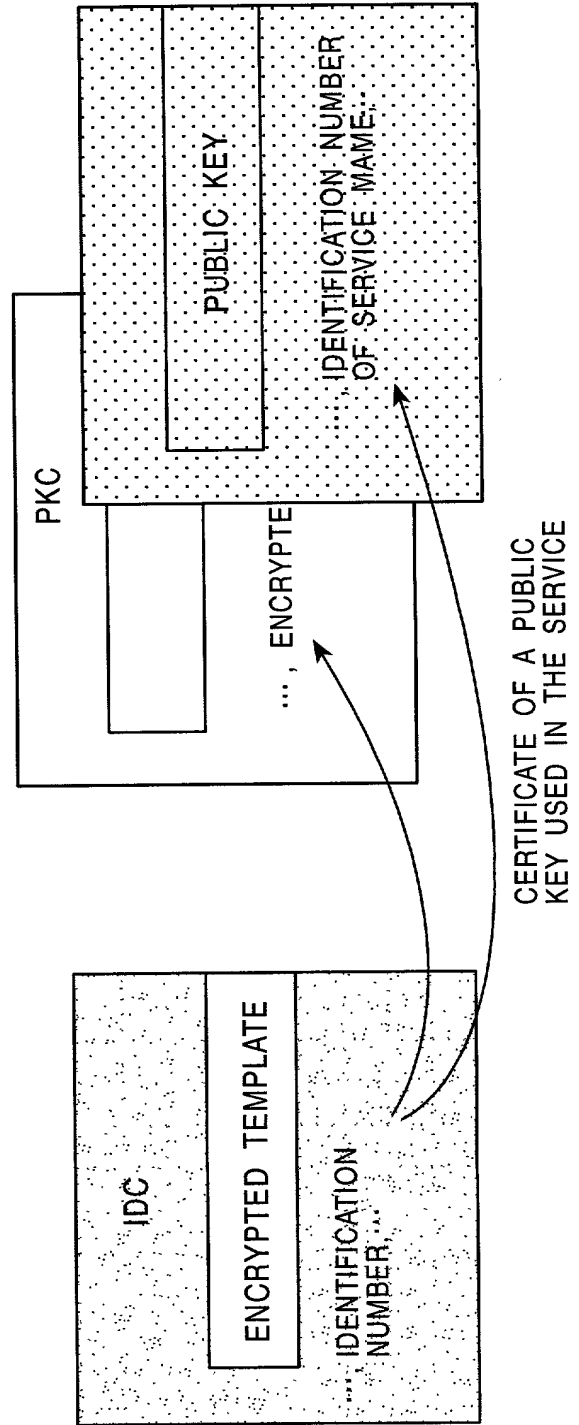


FIG. 50B



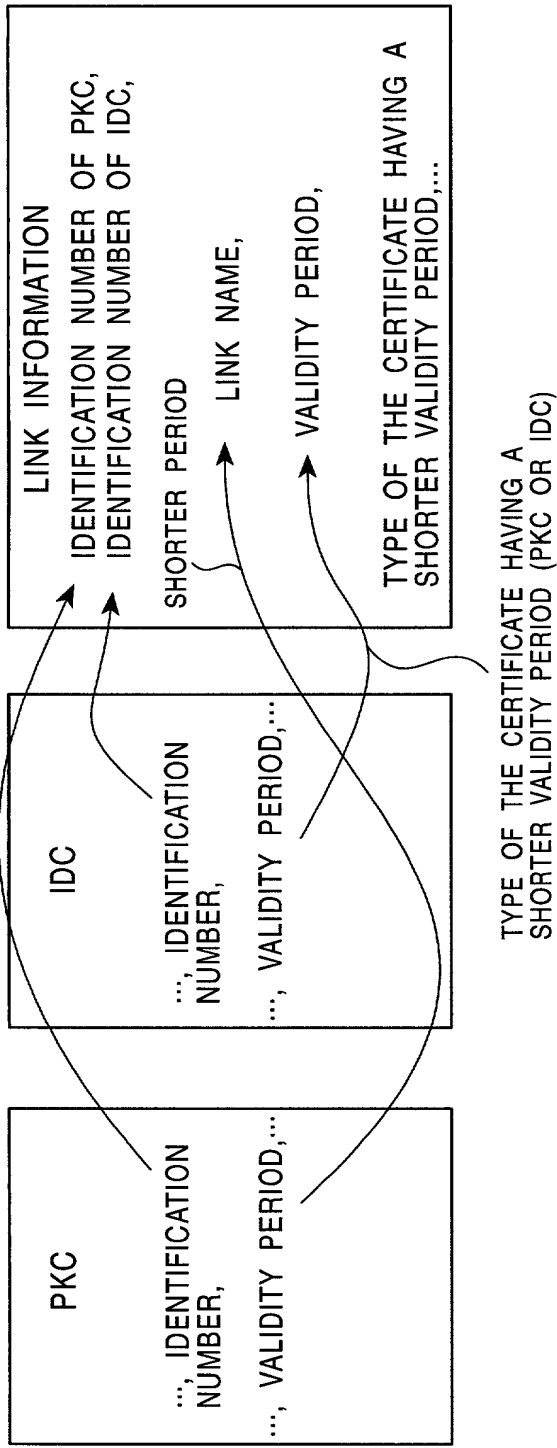


FIG. 51A

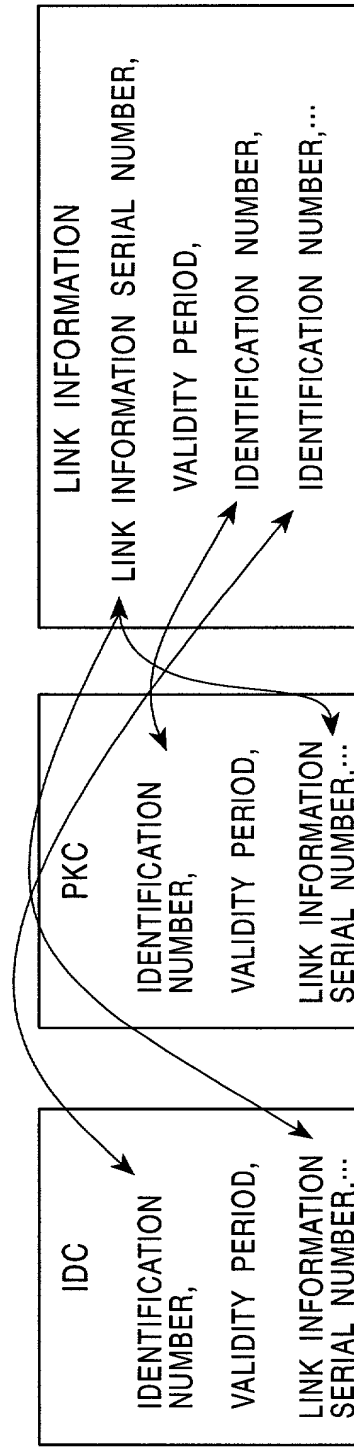


FIG. 51B

FIG. 52A

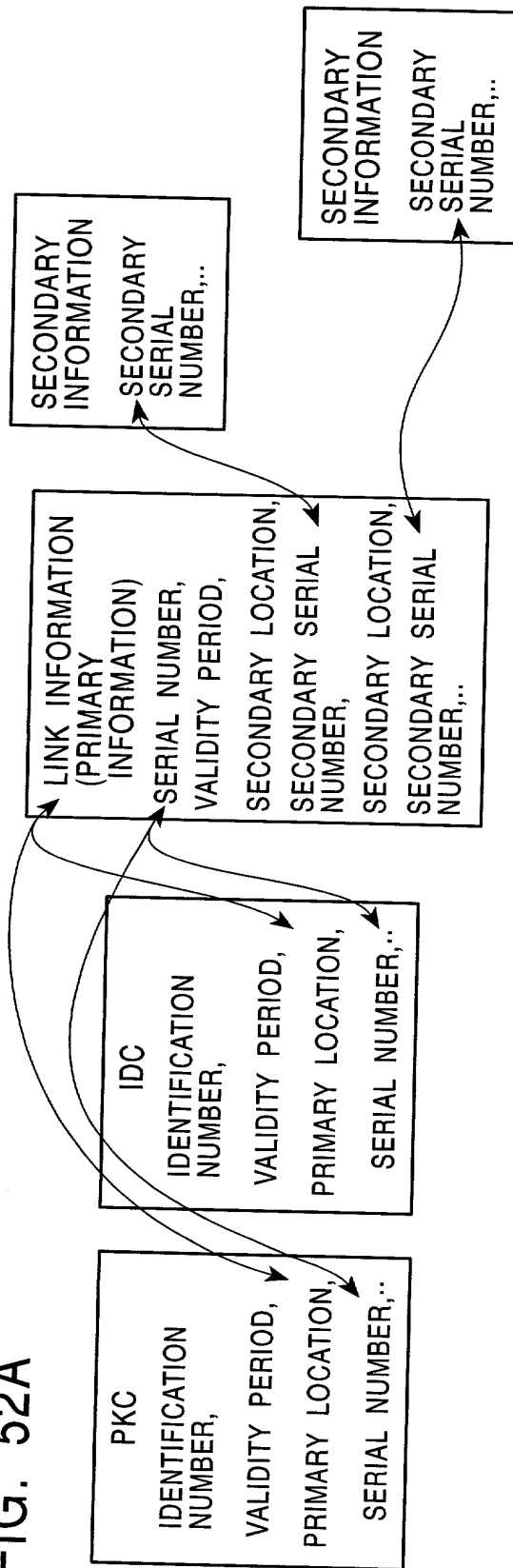


FIG. 52B

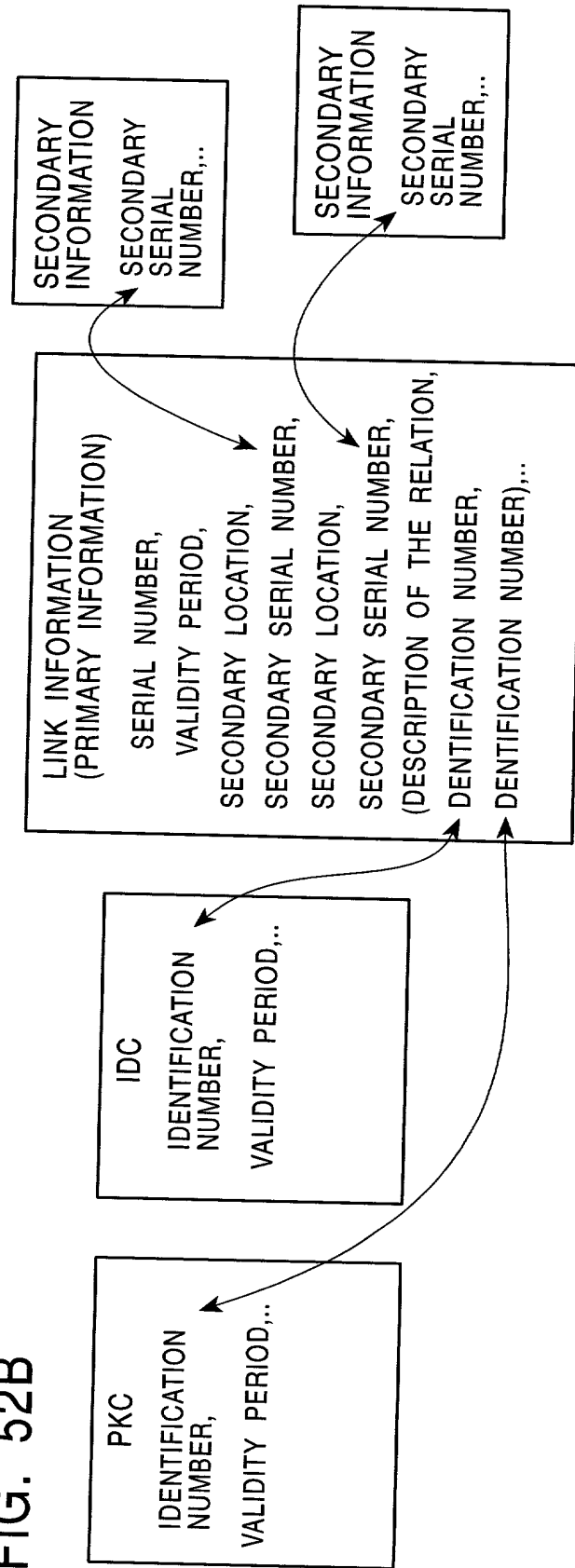


FIG. 53

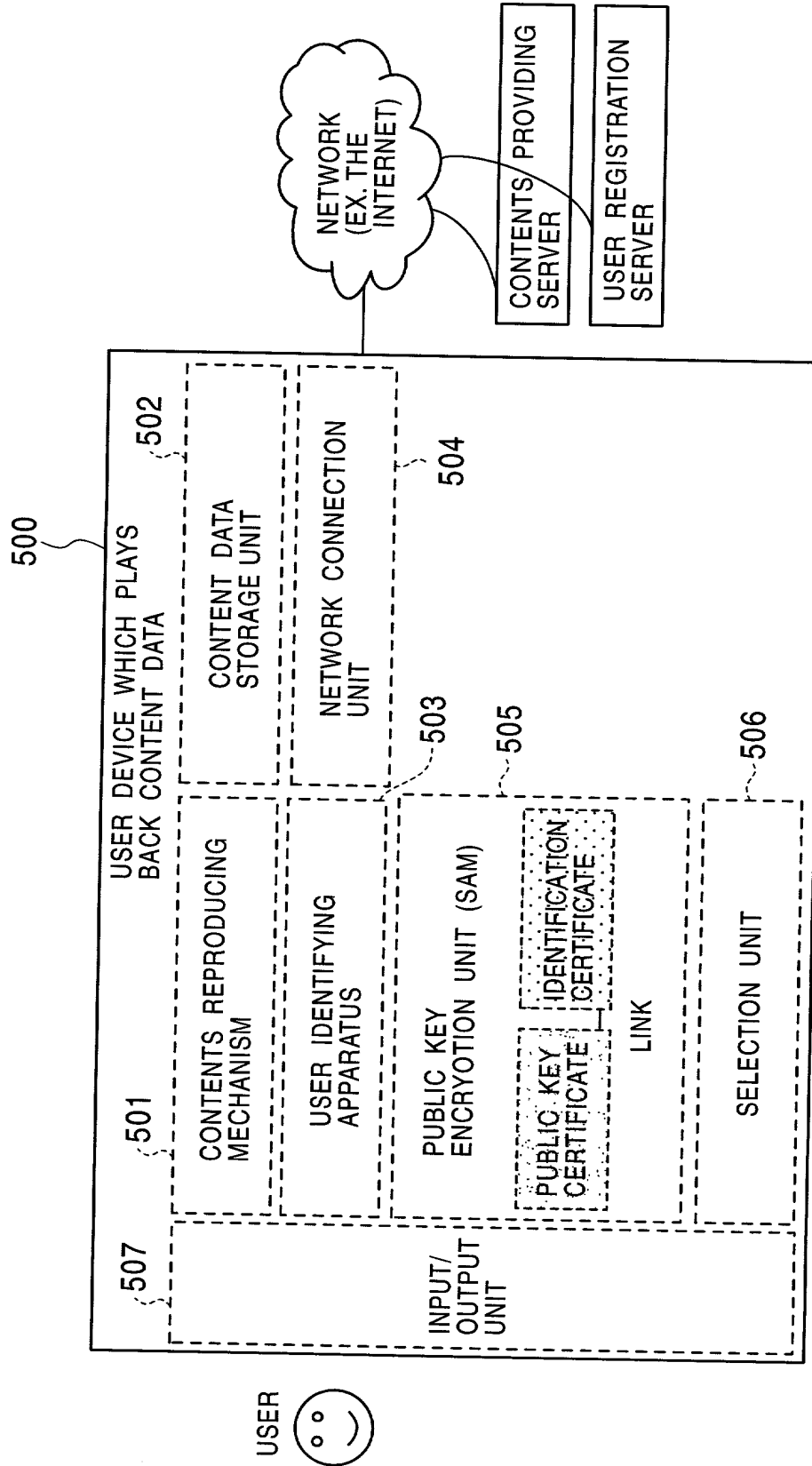


FIG. 54

## PRECONDITIONS:

- IDC AND PKC HAVE BEEN ACQUIRED
- USER REGISTRATION IN THE CONTENTS PROVIDING SERVER HAS BEEN PERFORMED

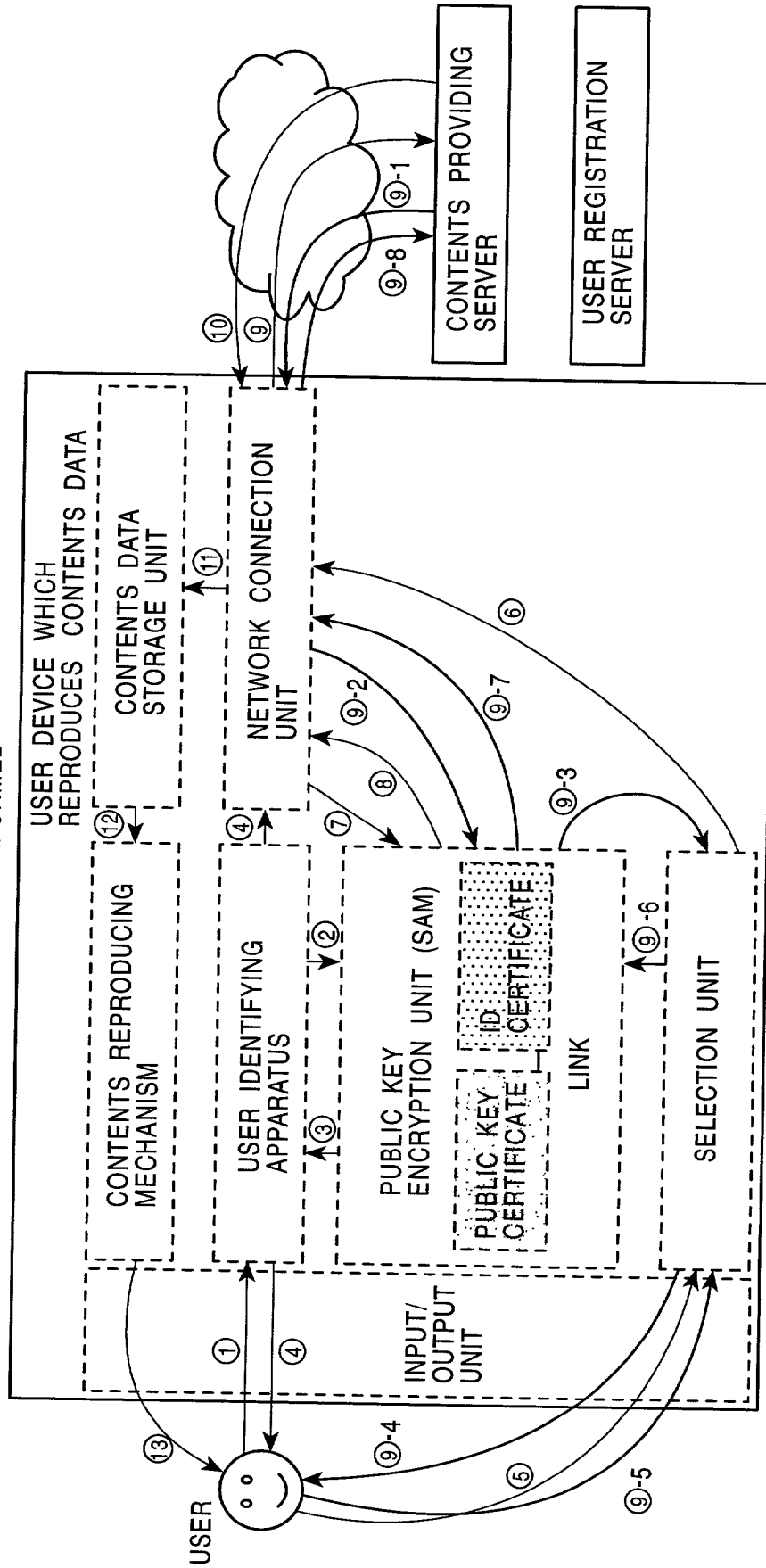




FIG. 55

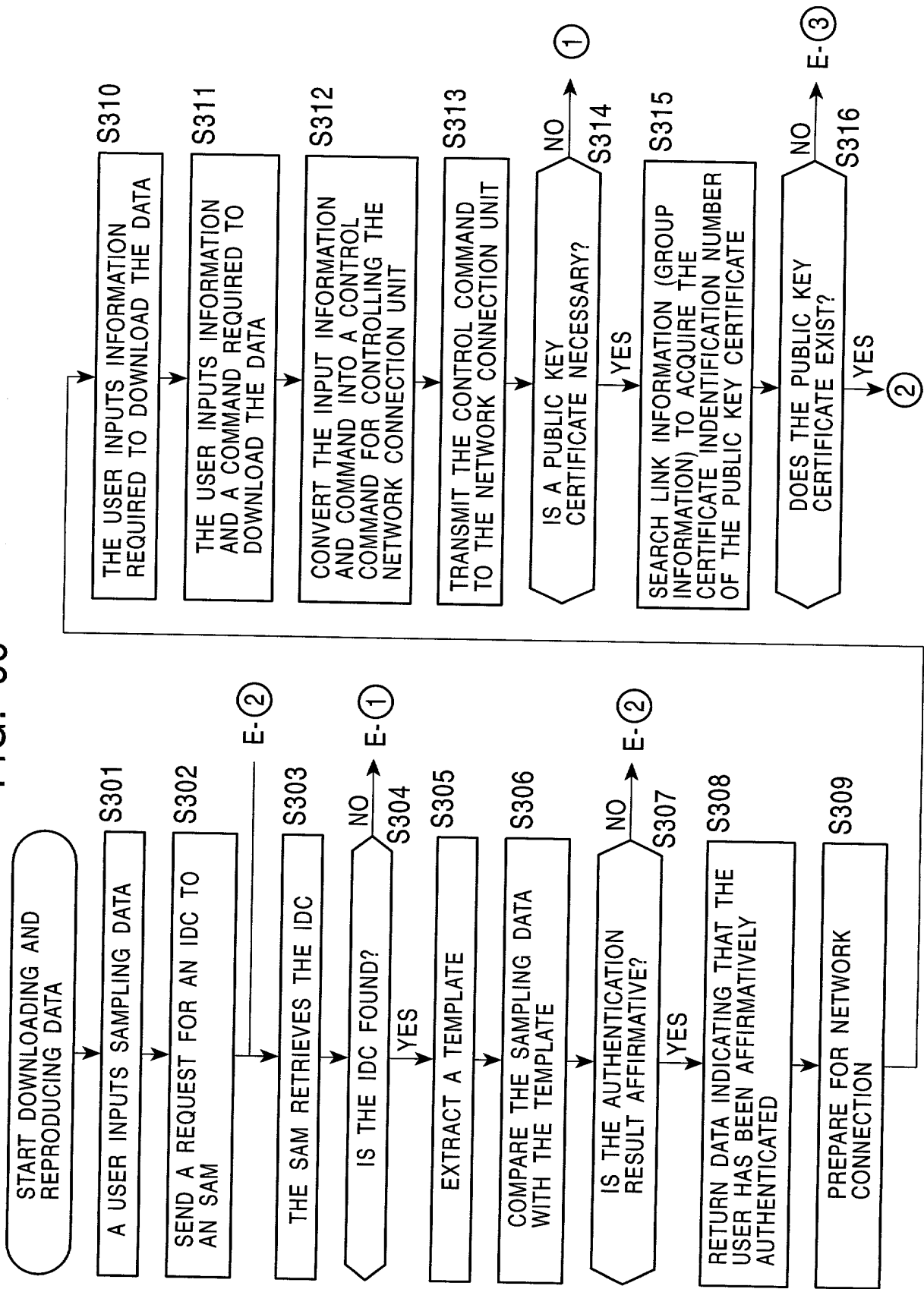


FIG. 56

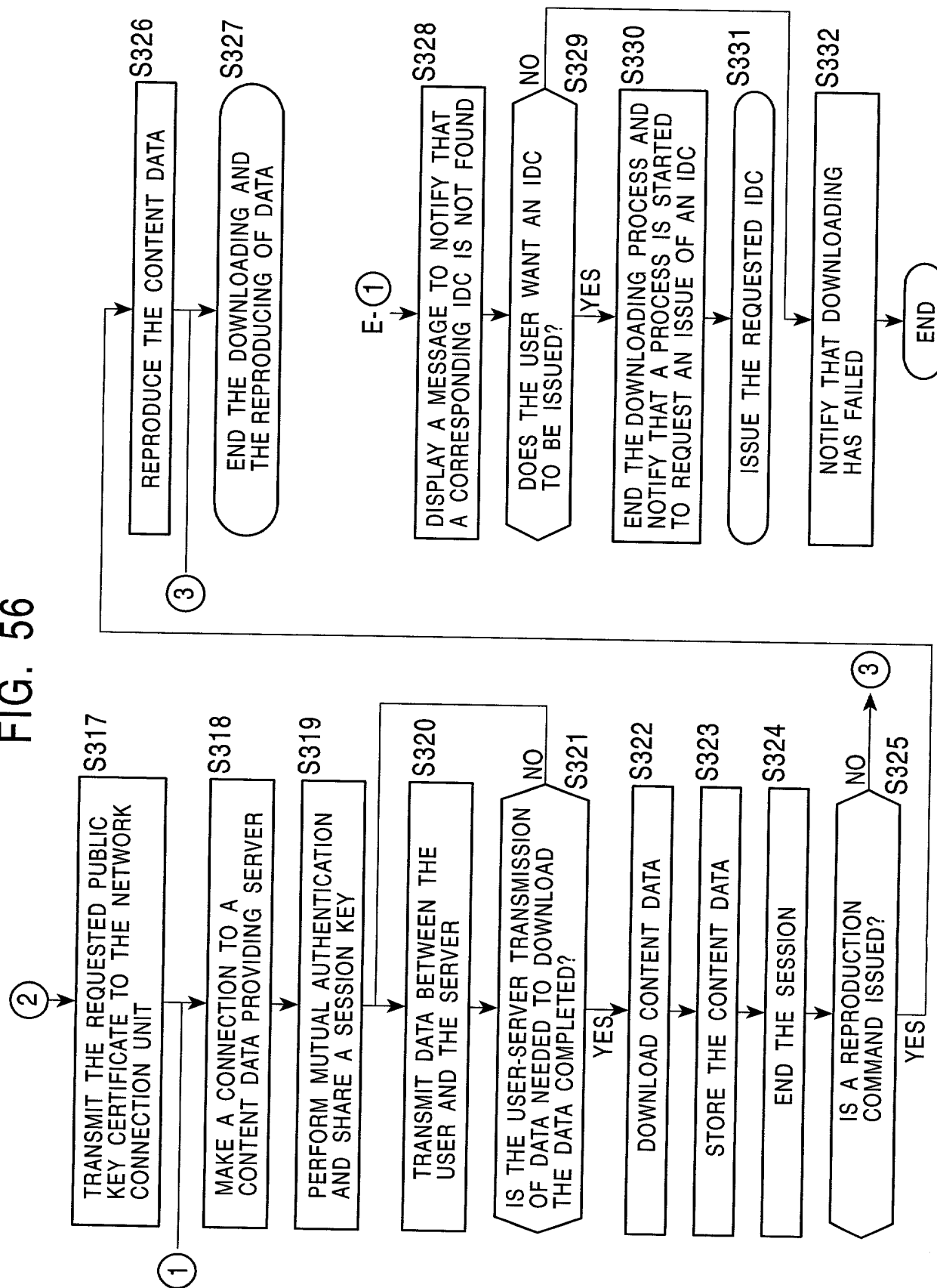


FIG. 57

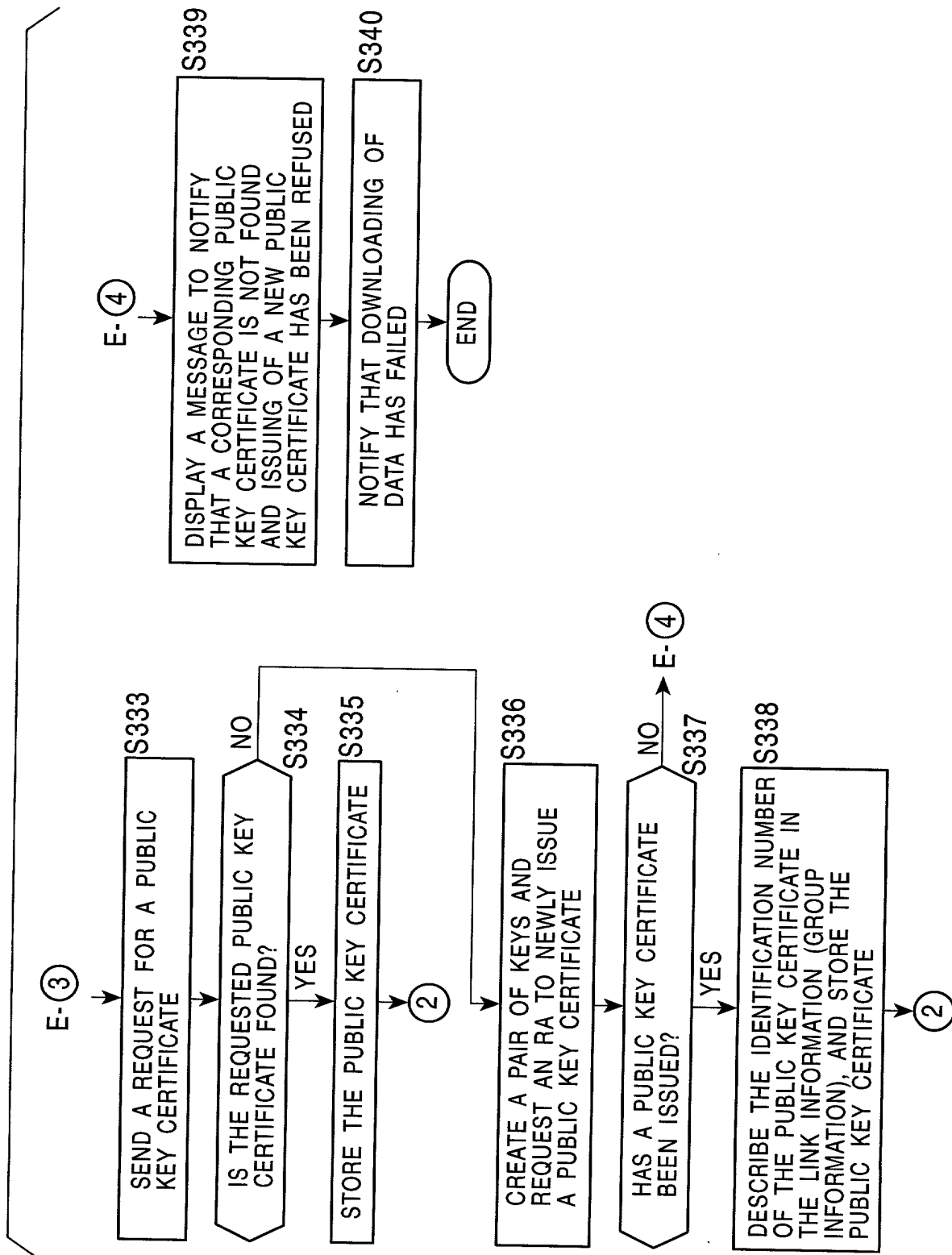


FIG. 58

PRECONDITION:

- IDC AND PKC HAVE BEEN ACQUIRED

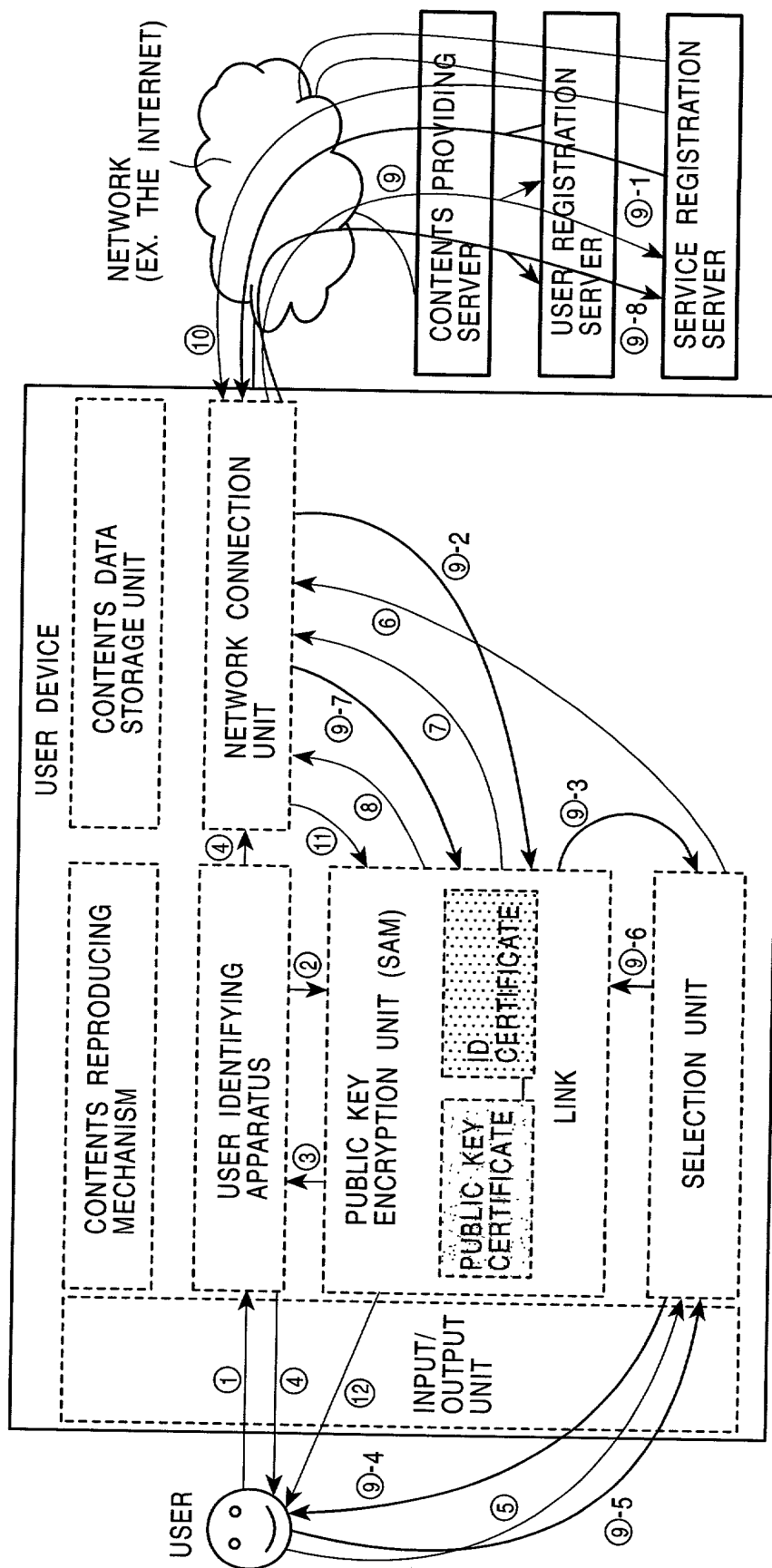


FIG. 59

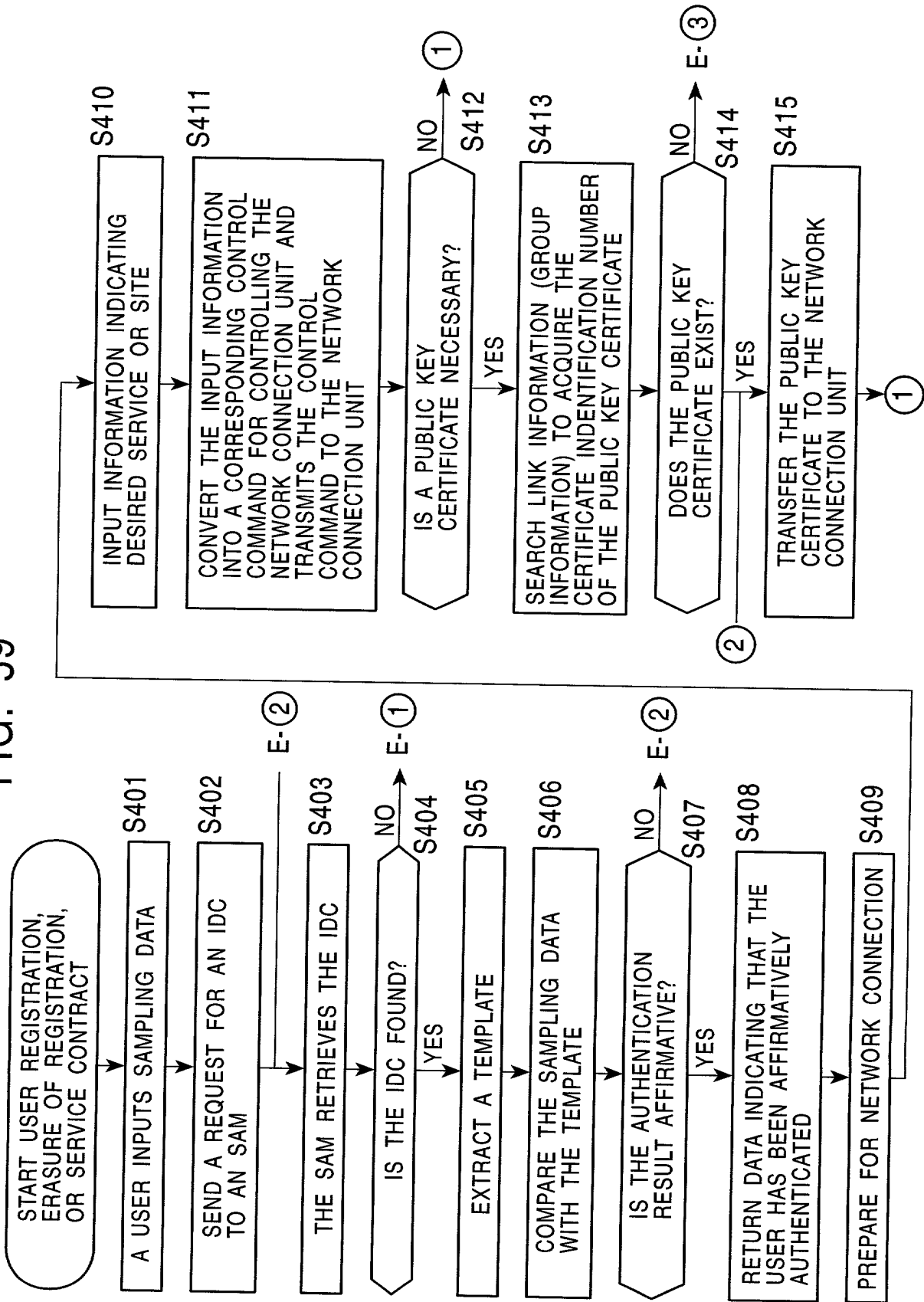


FIG. 60

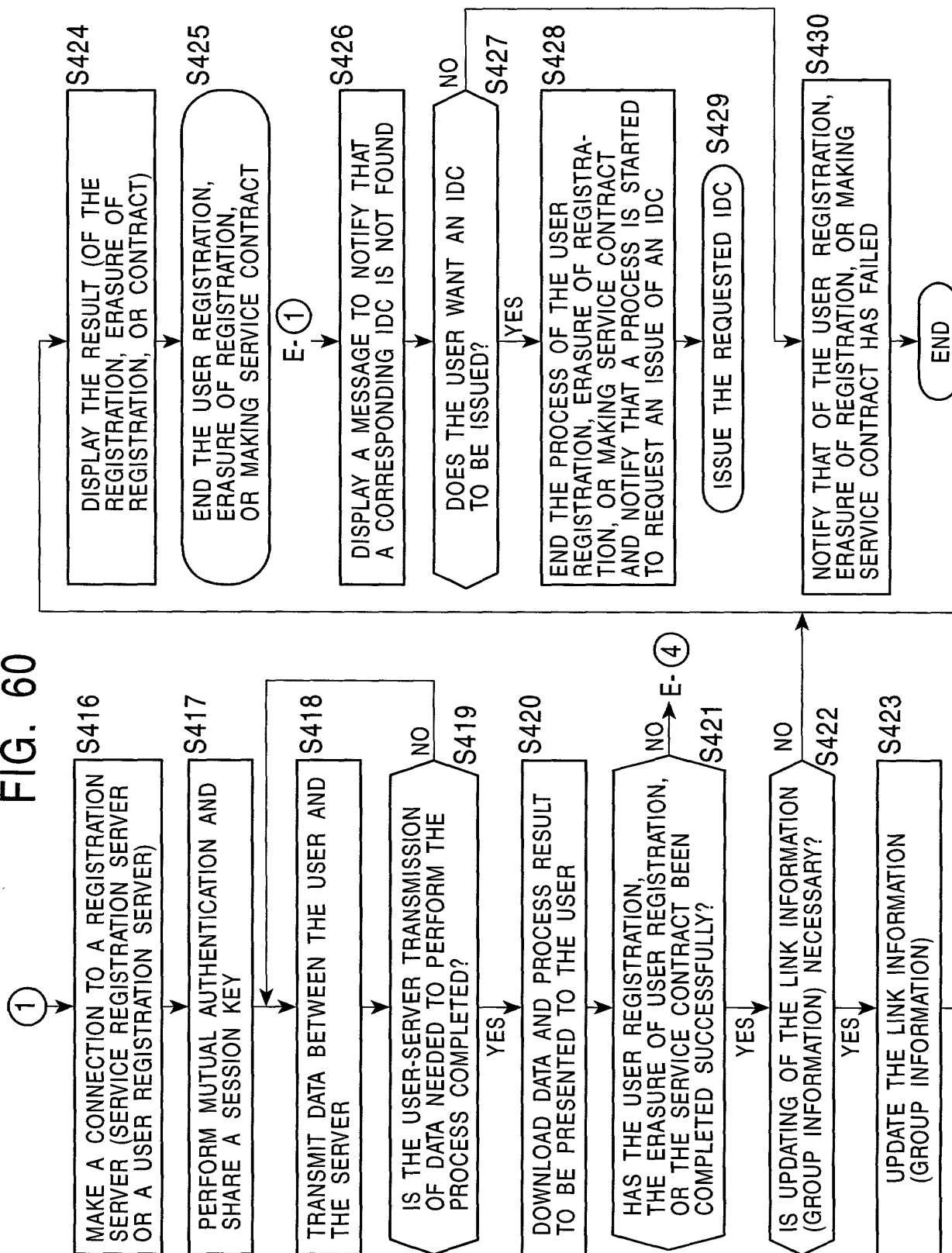


FIG. 61

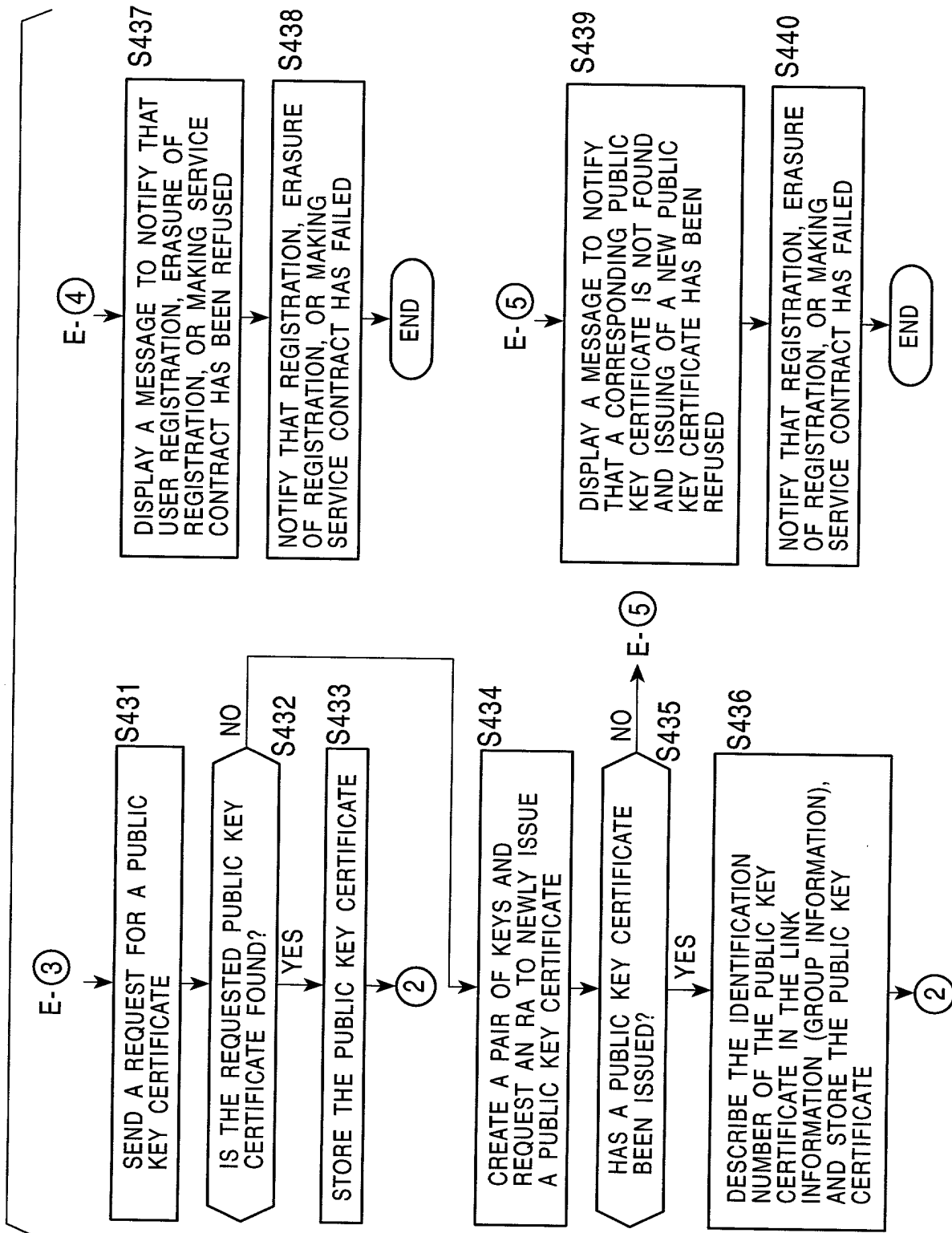


FIG. 62

## PRECONDITIONS:

- AN IDC OF INTEREST HAS NOT BEEN REGISTERED IN THE USER DEVICE
- THE USER DEVICE HAS NEITHER A PKC NOR A PAIR OF KEYS BUT THE USER DEVICE CAN CREATE THEM
- AN OFF-LINE PROCEDURE NEEDED TO ISSUE AN IDC HAS BEEN PERFORMED, AND INFORMATION (PIN, TEMPLATE, OR SIGNATURE ENCRYPTED USING A PRIVATE KEY) USED TO CHECK WHETHER A TEMPLATE SUPPLIER IS IDENTICAL TO AN APPLICANT HAS BEEN DETERMINED

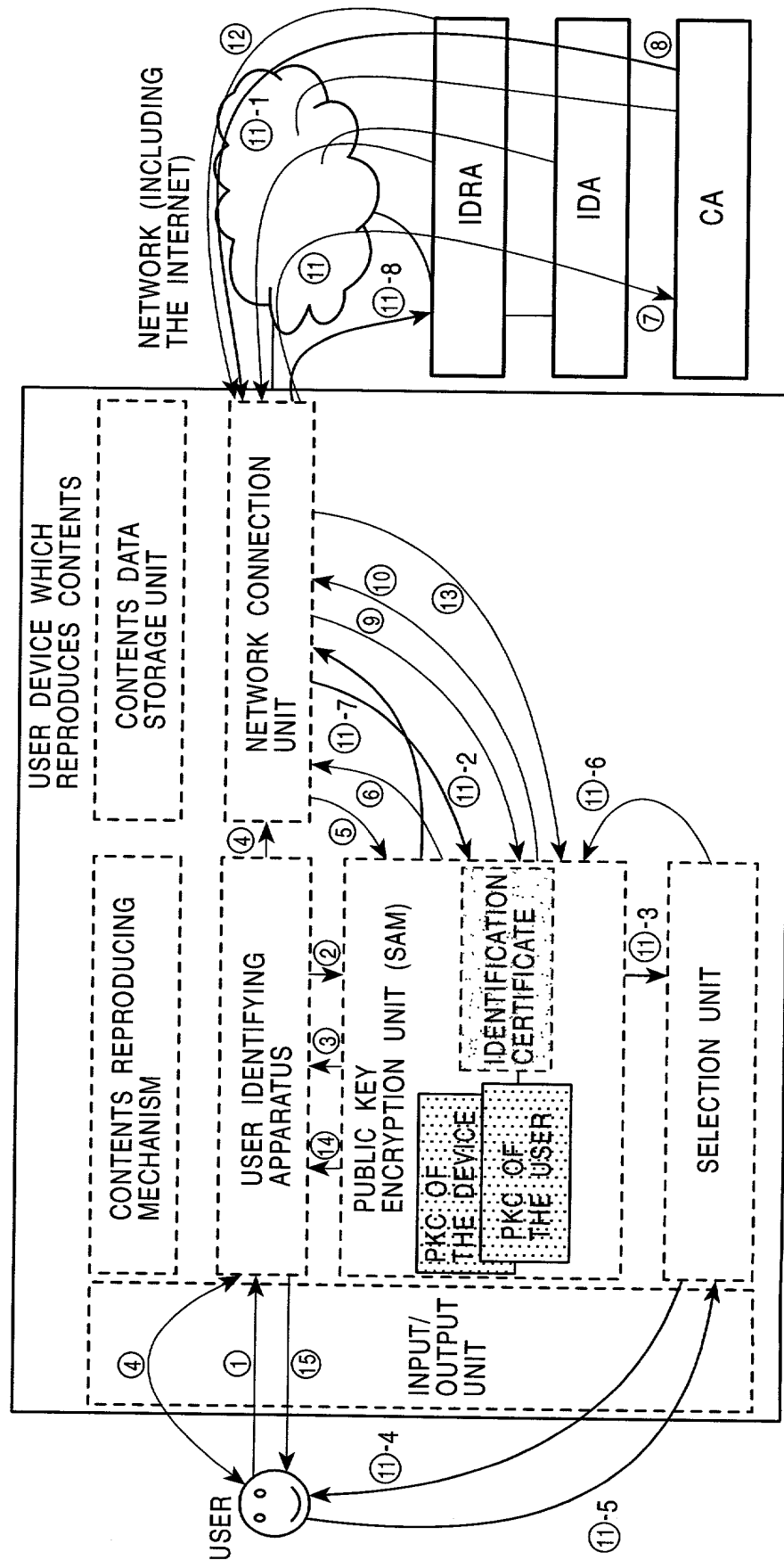




FIG. 63

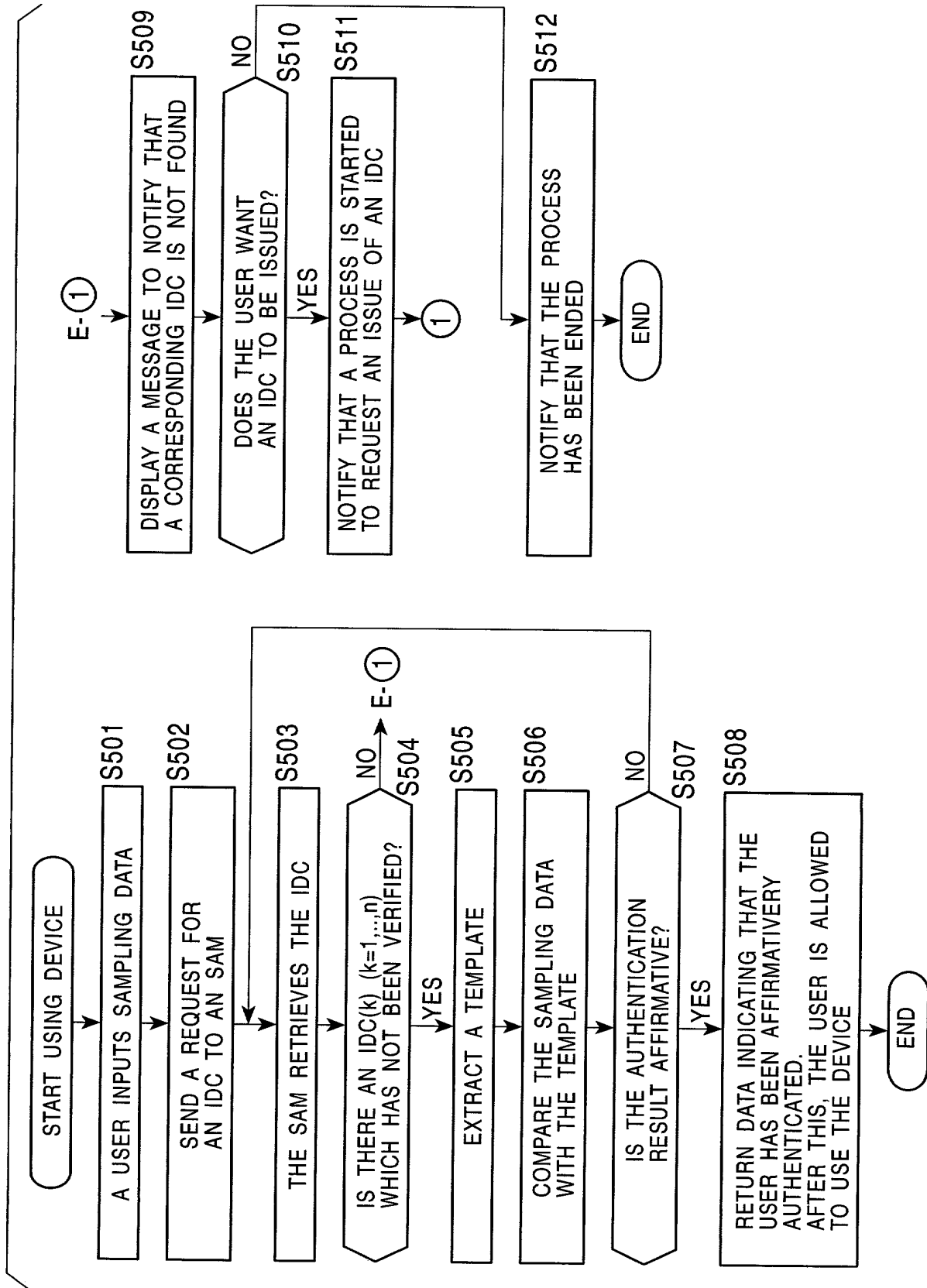




FIG. 65

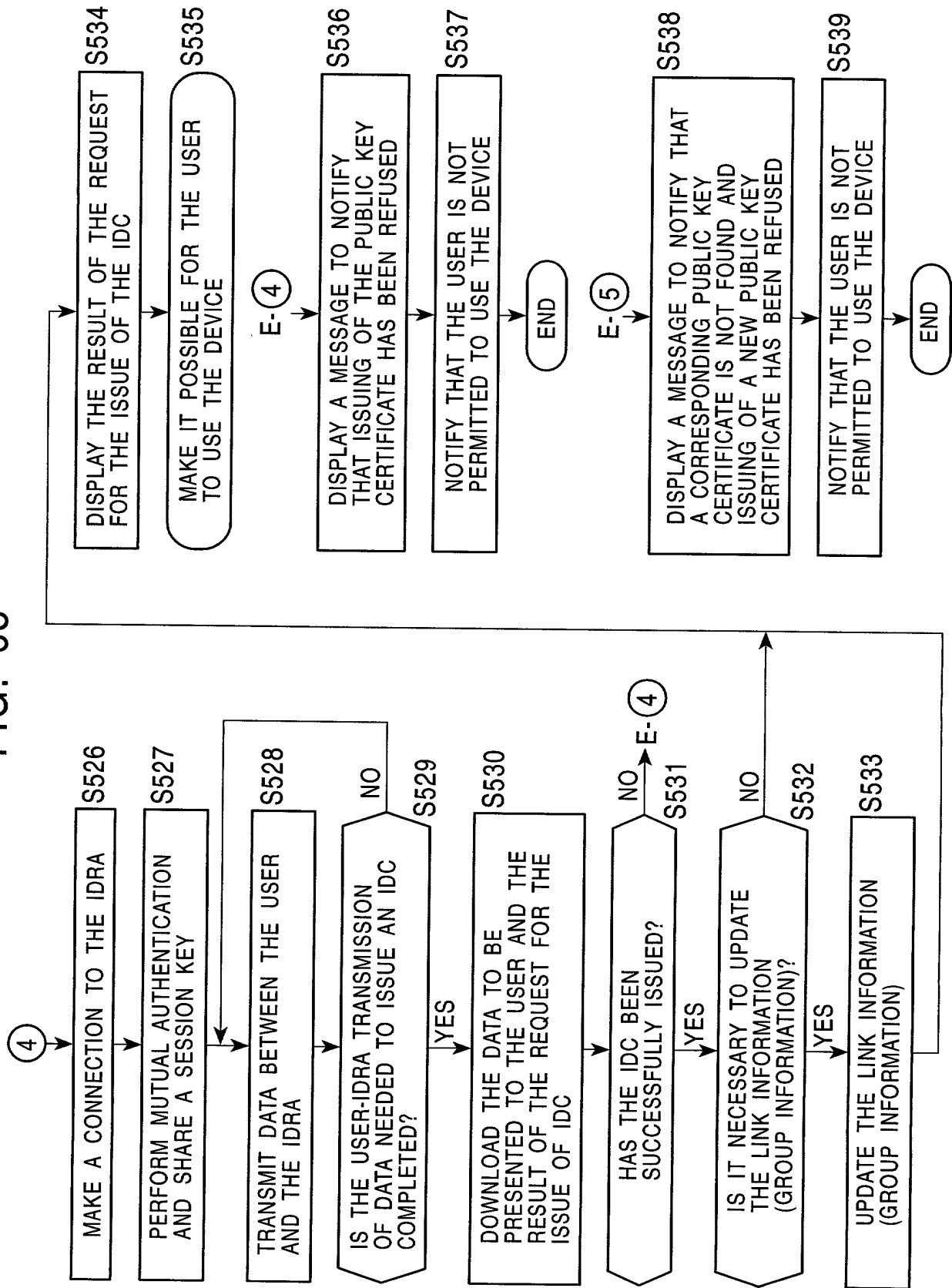


FIG. 66

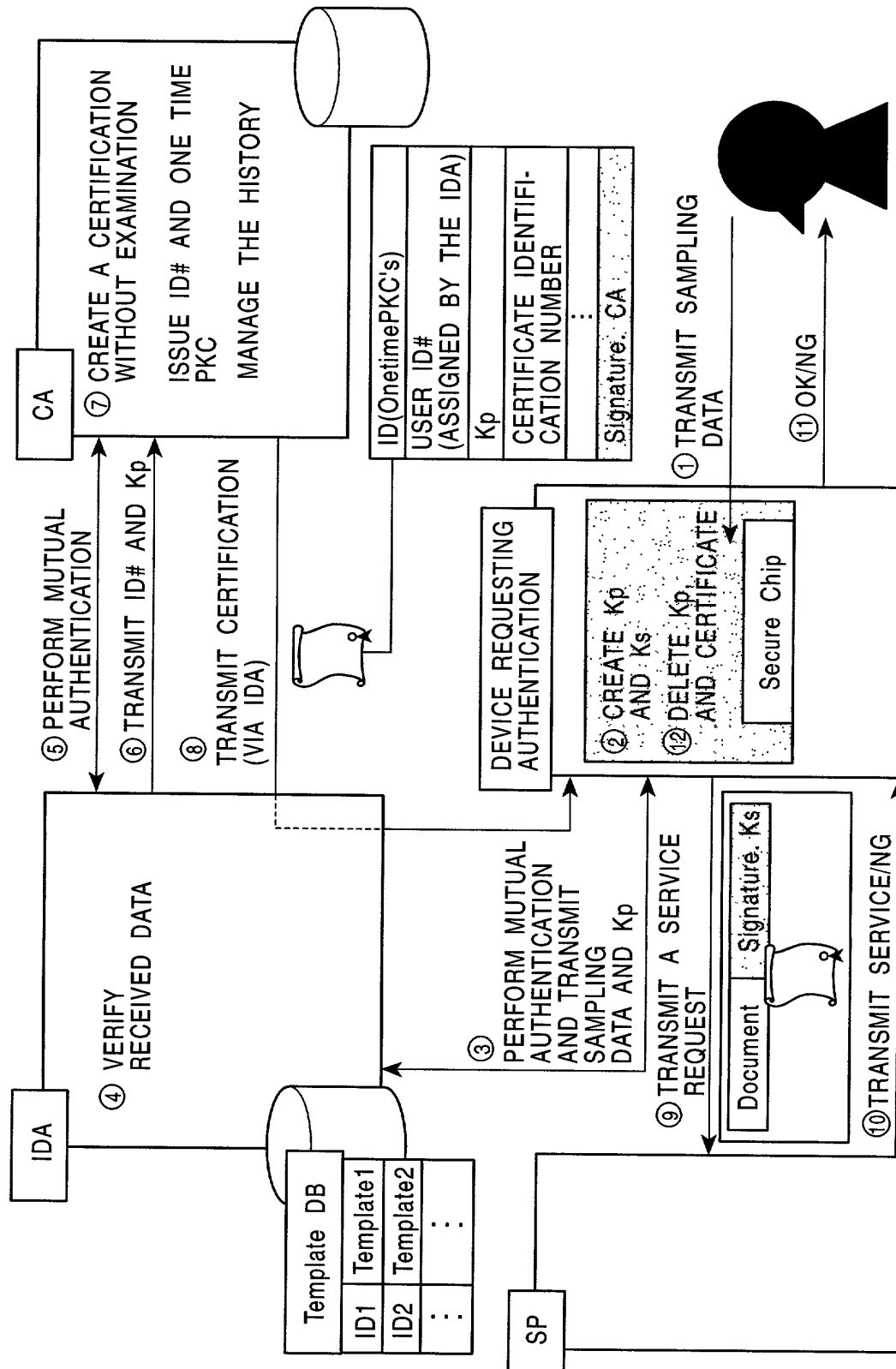


FIG. 67

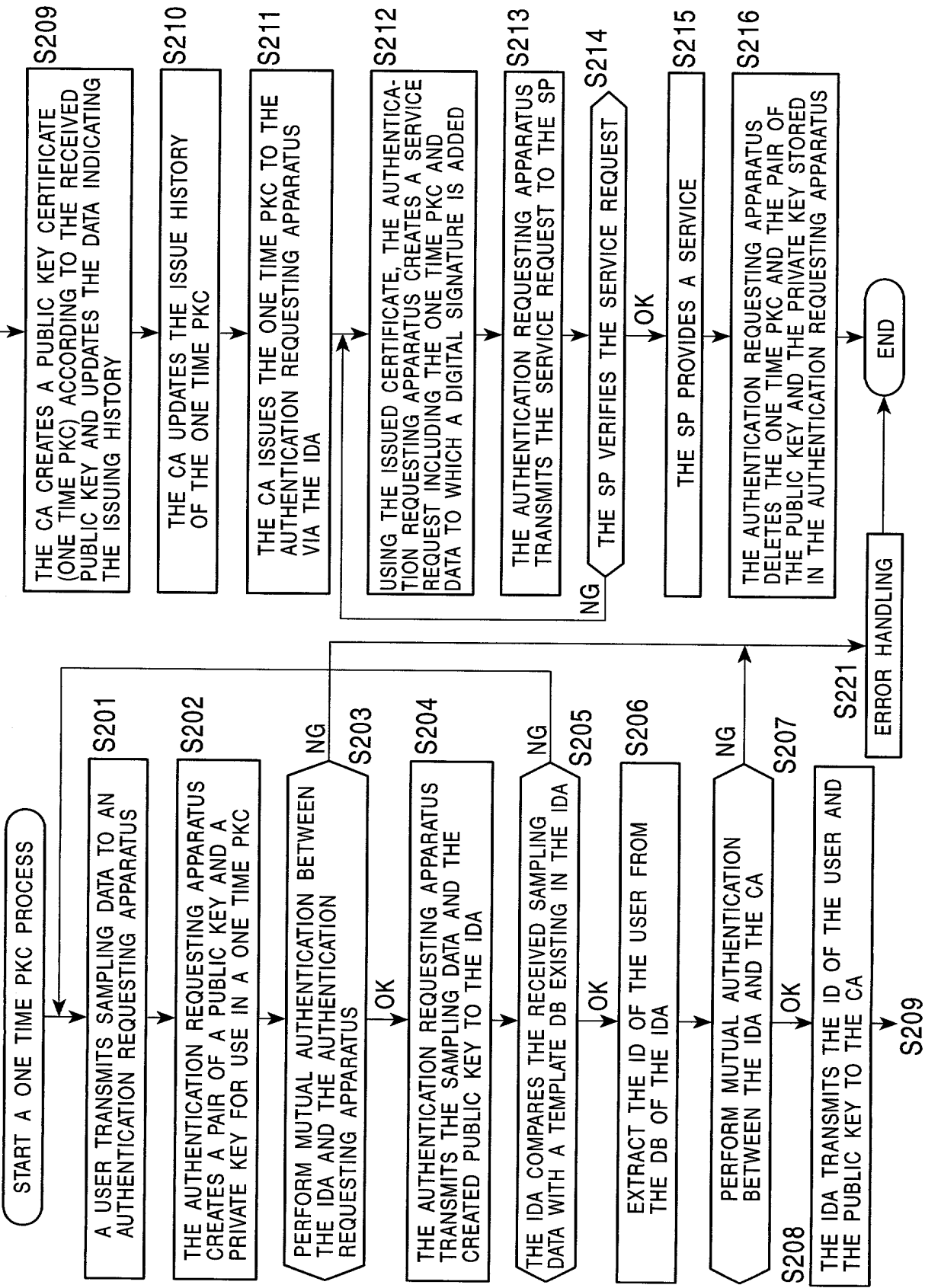


FIG. 68

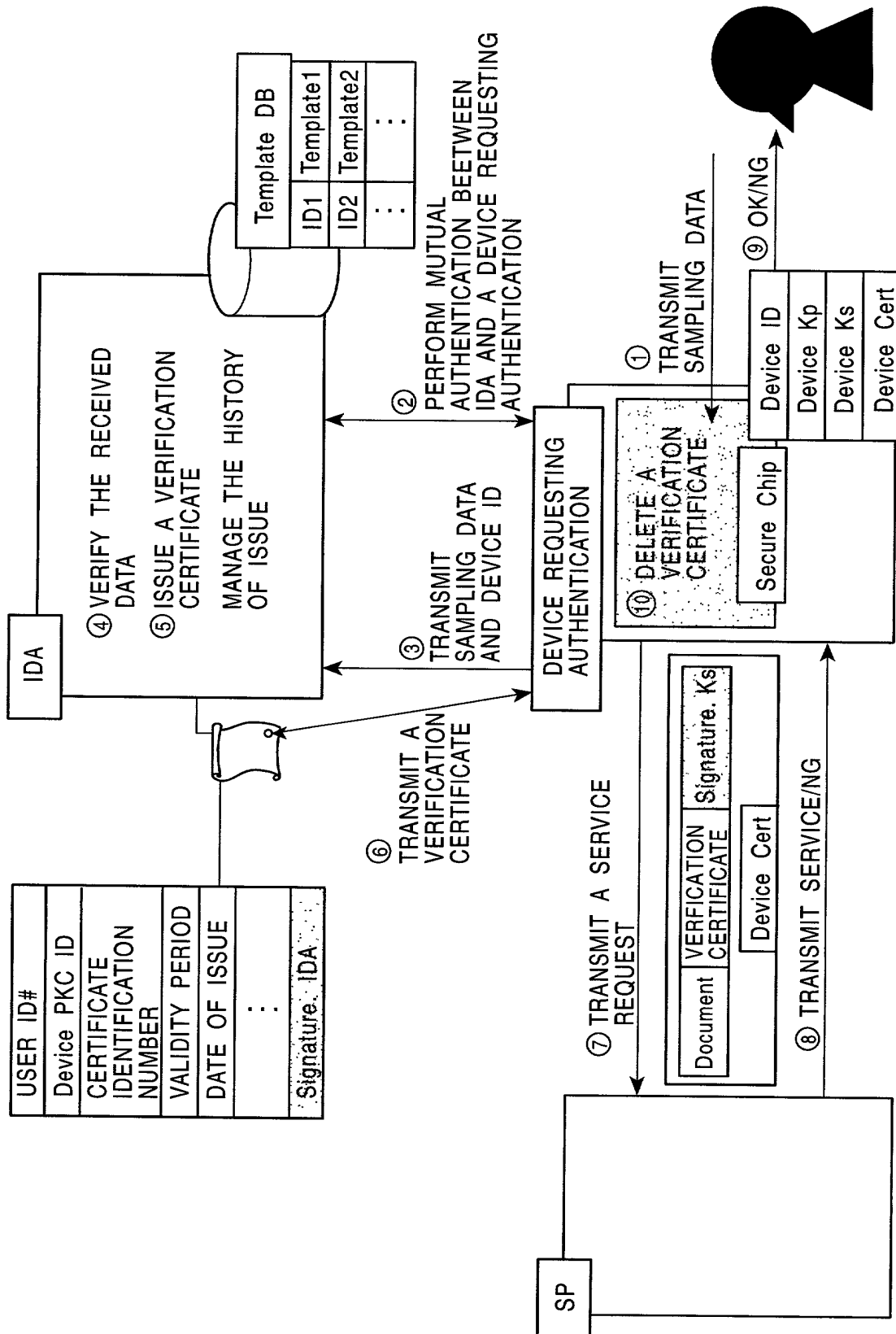


FIG. 69

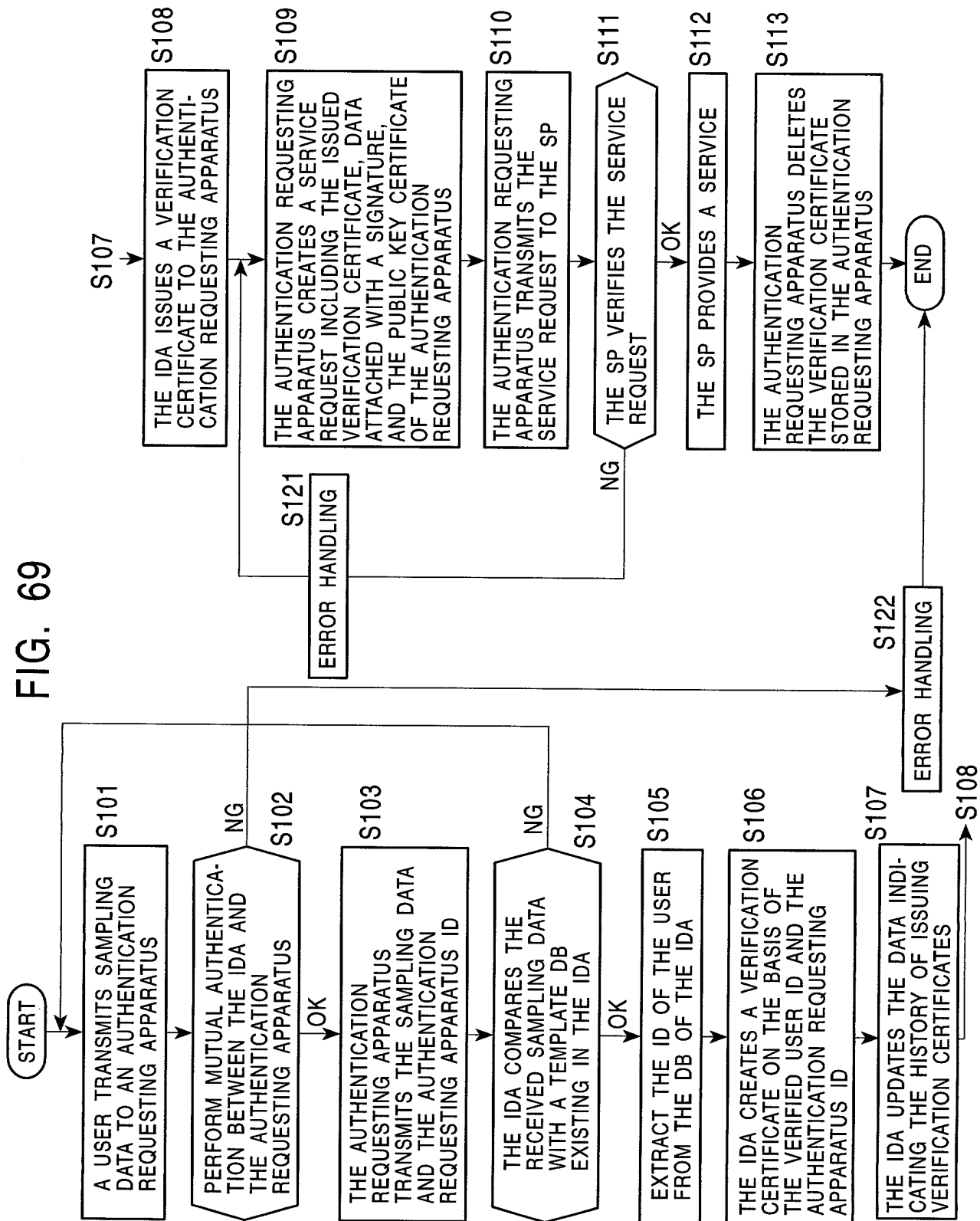


FIG. 70

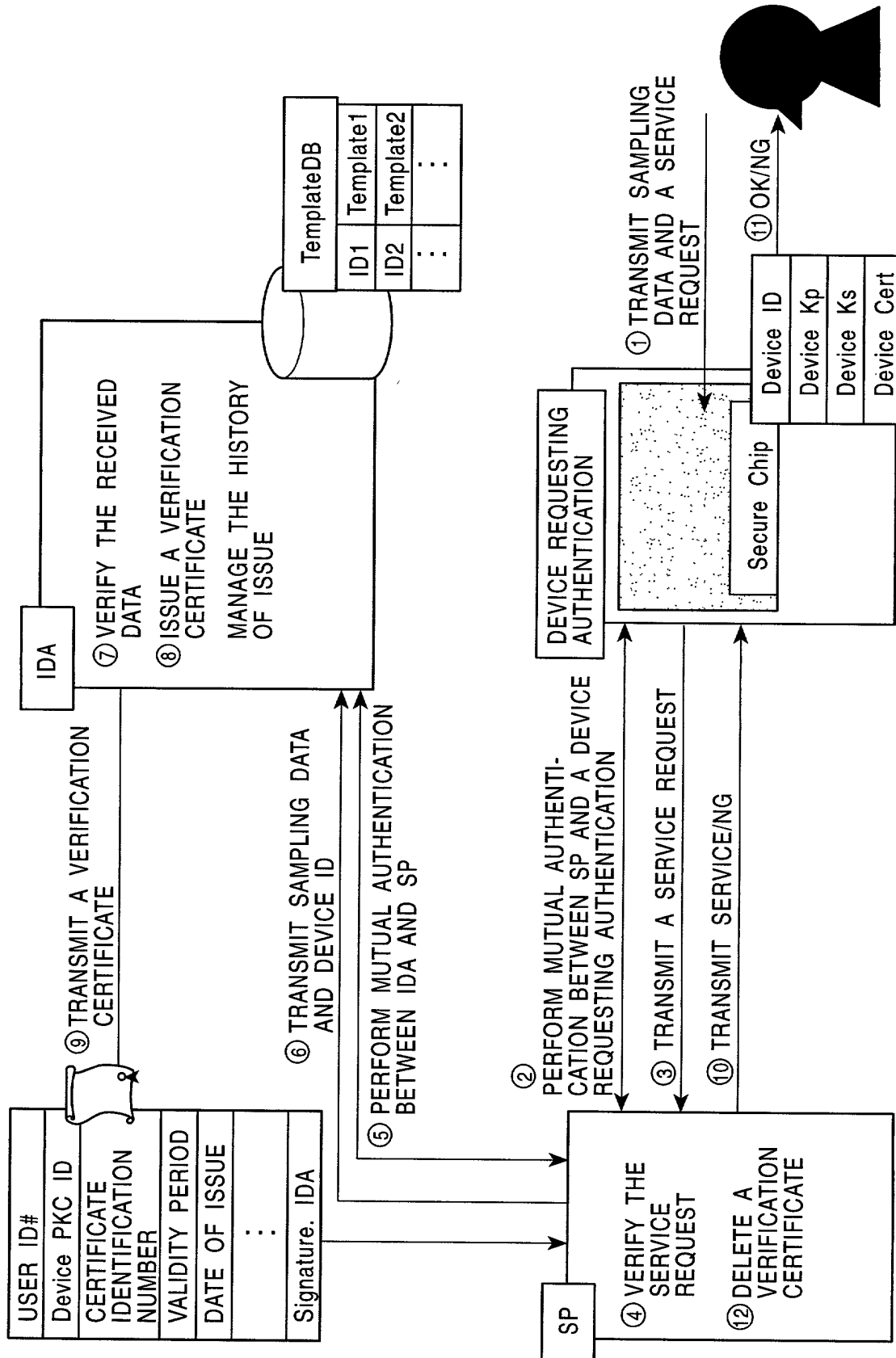




FIG. 71

	Item	Description
Indispensable Items	Version	Version
	Serial Number	Identification Number
	signature algorithm Identifier	Signature algorithm
	algorithm parameters	Algorithm Parameters
	Issuer	Identification authority name (in the form of a distinguished name)
	Validity notBefore notAfter	Validity period • Start date • Expiration date
	Subject	Subject Name (in a DN form)
	subject IDA Info subject IDA serial Number subject IDA Unique ID	Information about the identification certificate of the subject • Certificate number of the identification certificate of the subject • Subject unique ID of the identification certificate of the subject
Indispensable	subject PKC info subject PKC serial Number subject PKC Unique ID	Information about the public key certificate of the subject • Certificate Number of the public key certificate of the subject • Subject unique ID of the public key certificate of the subject
	IDA Signature	Signature of IDA

FIG. 72

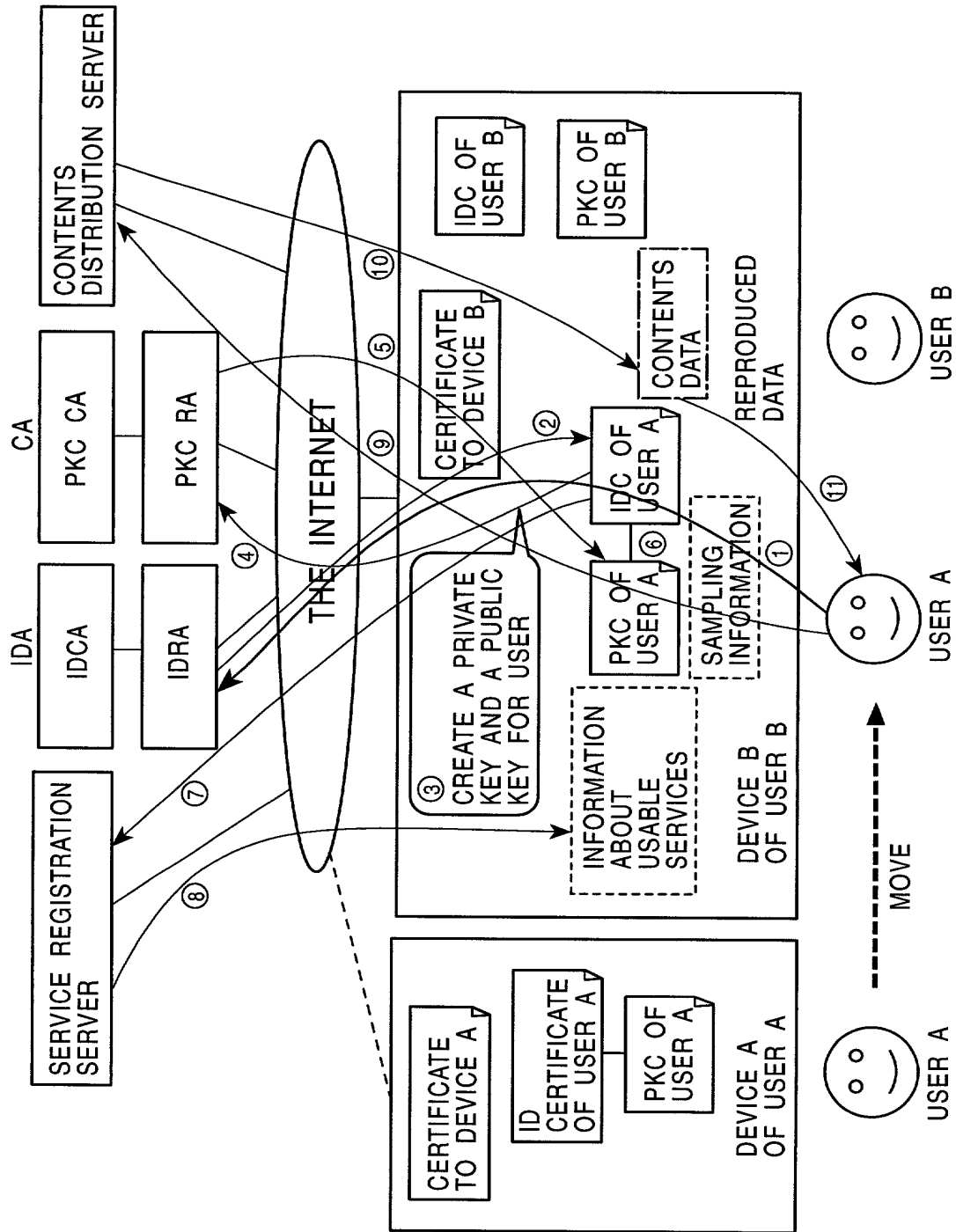


FIG. 73

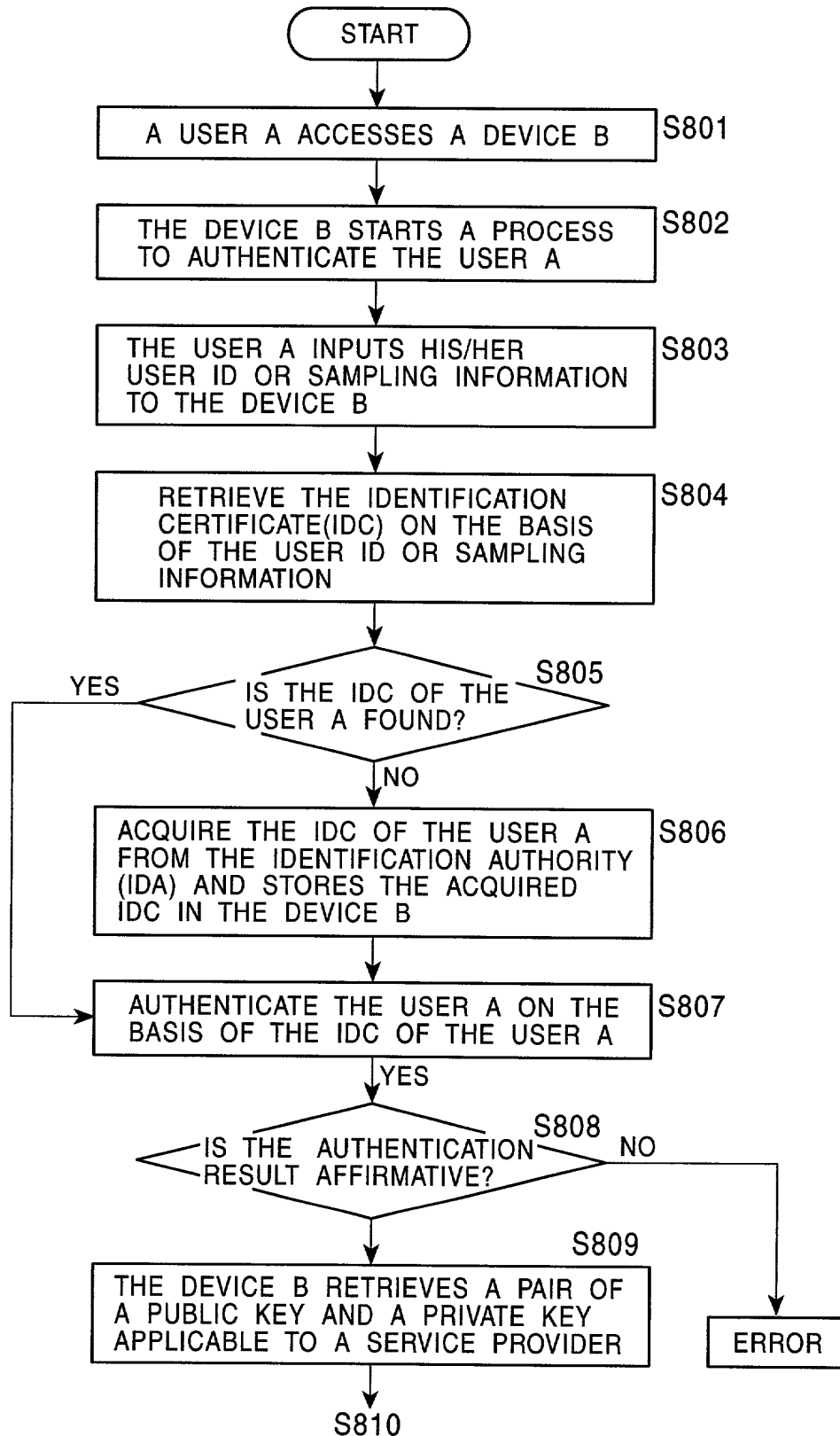


FIG. 74

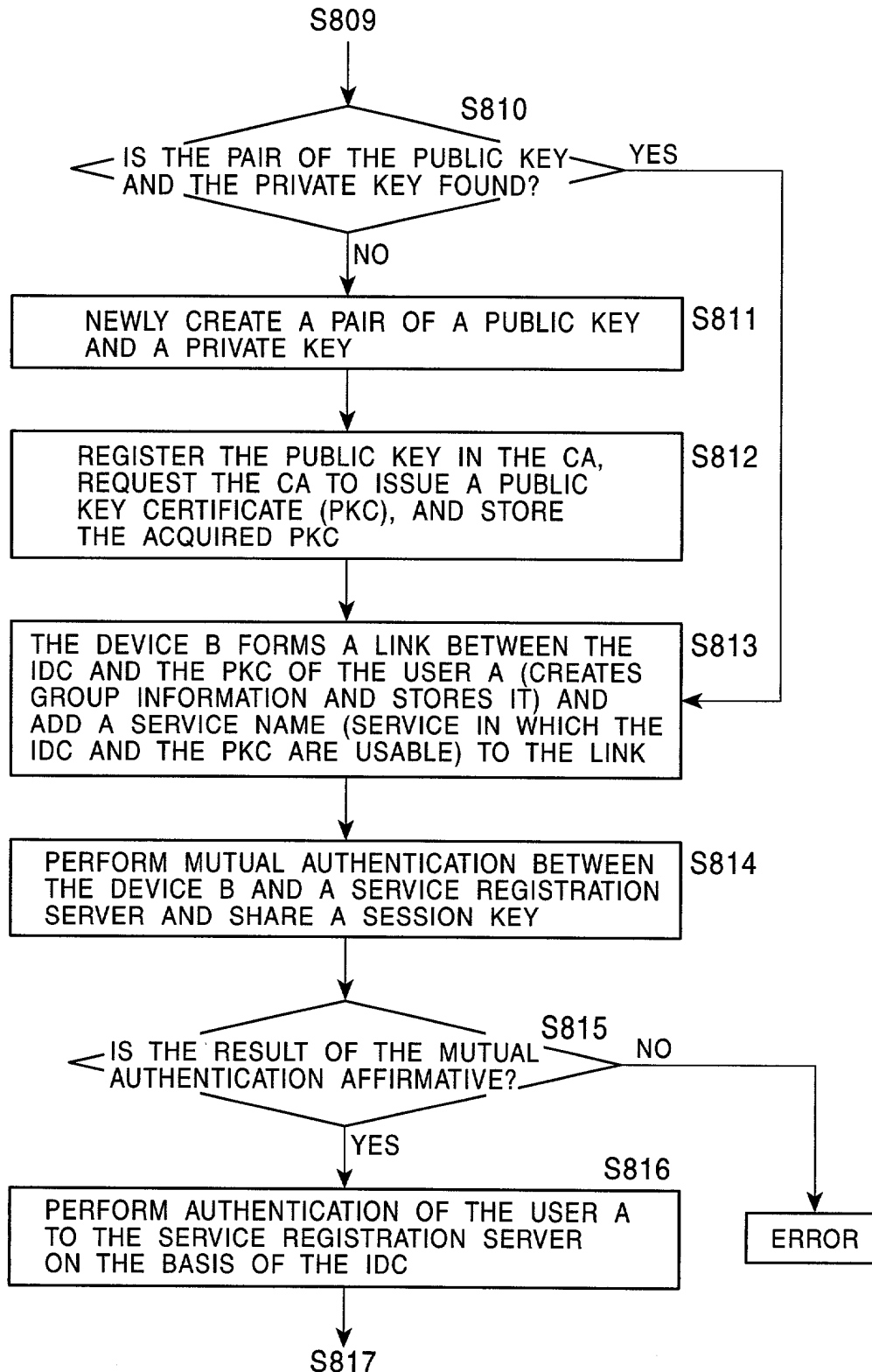


FIG. 75

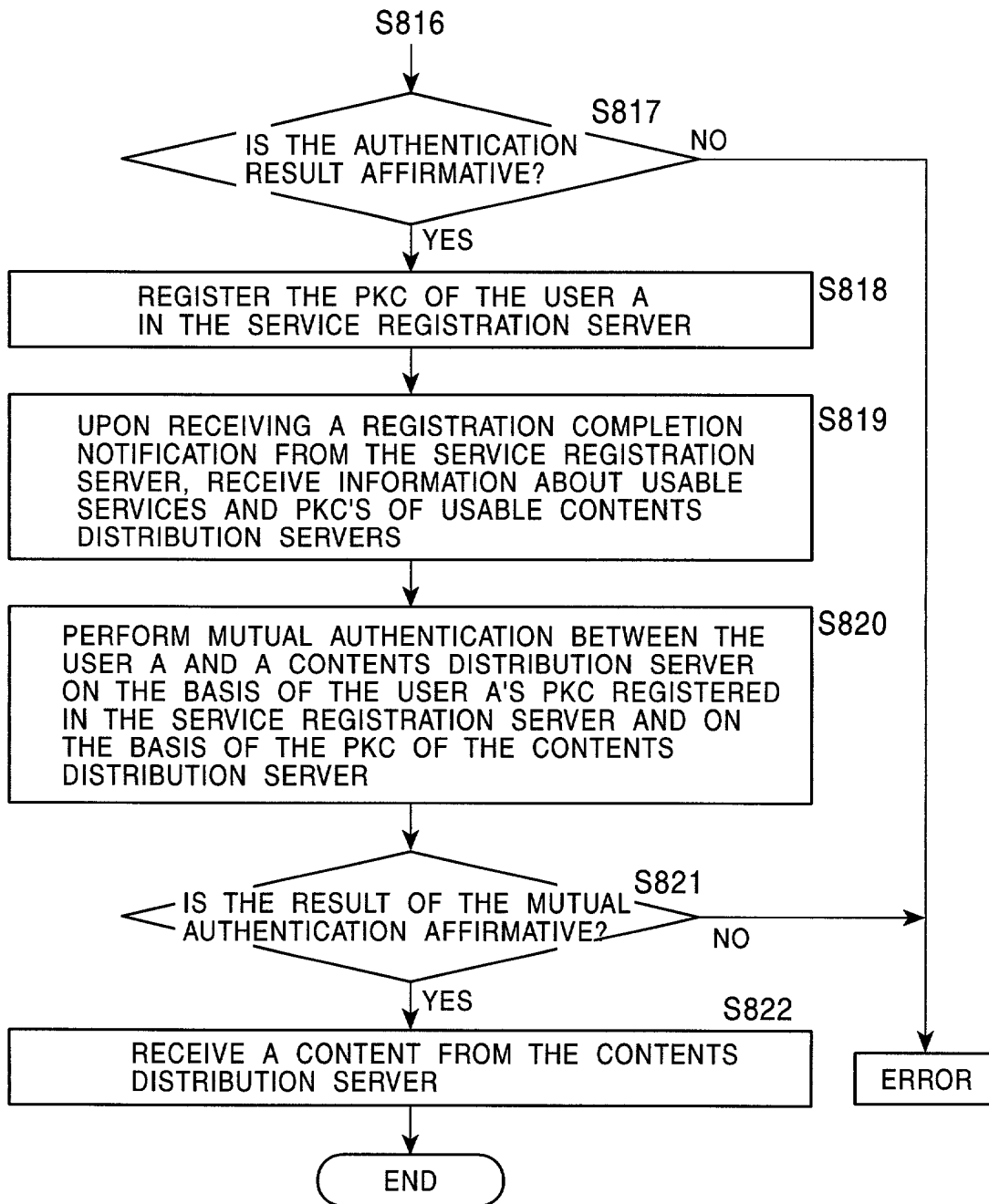


FIG. 76

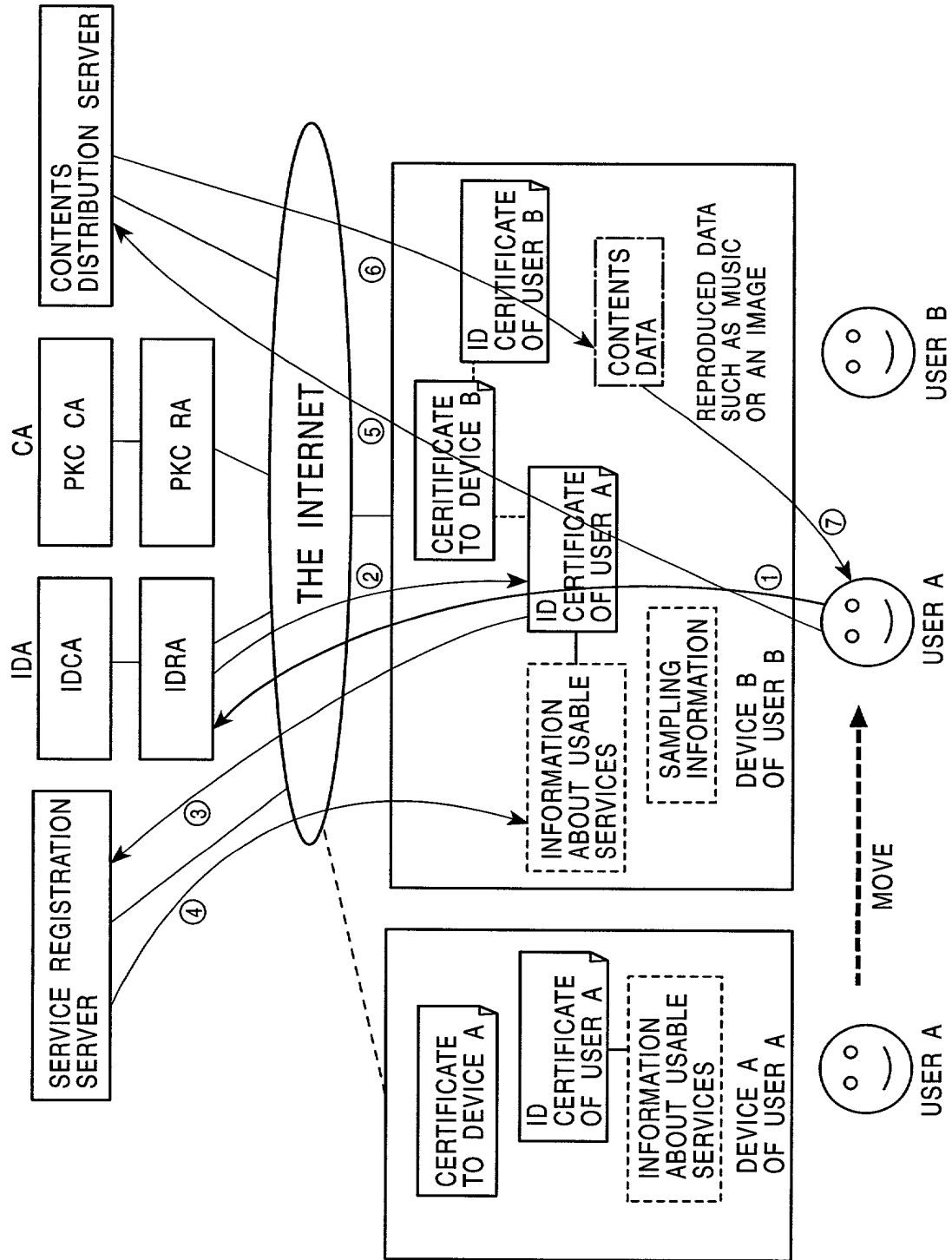


FIG. 77

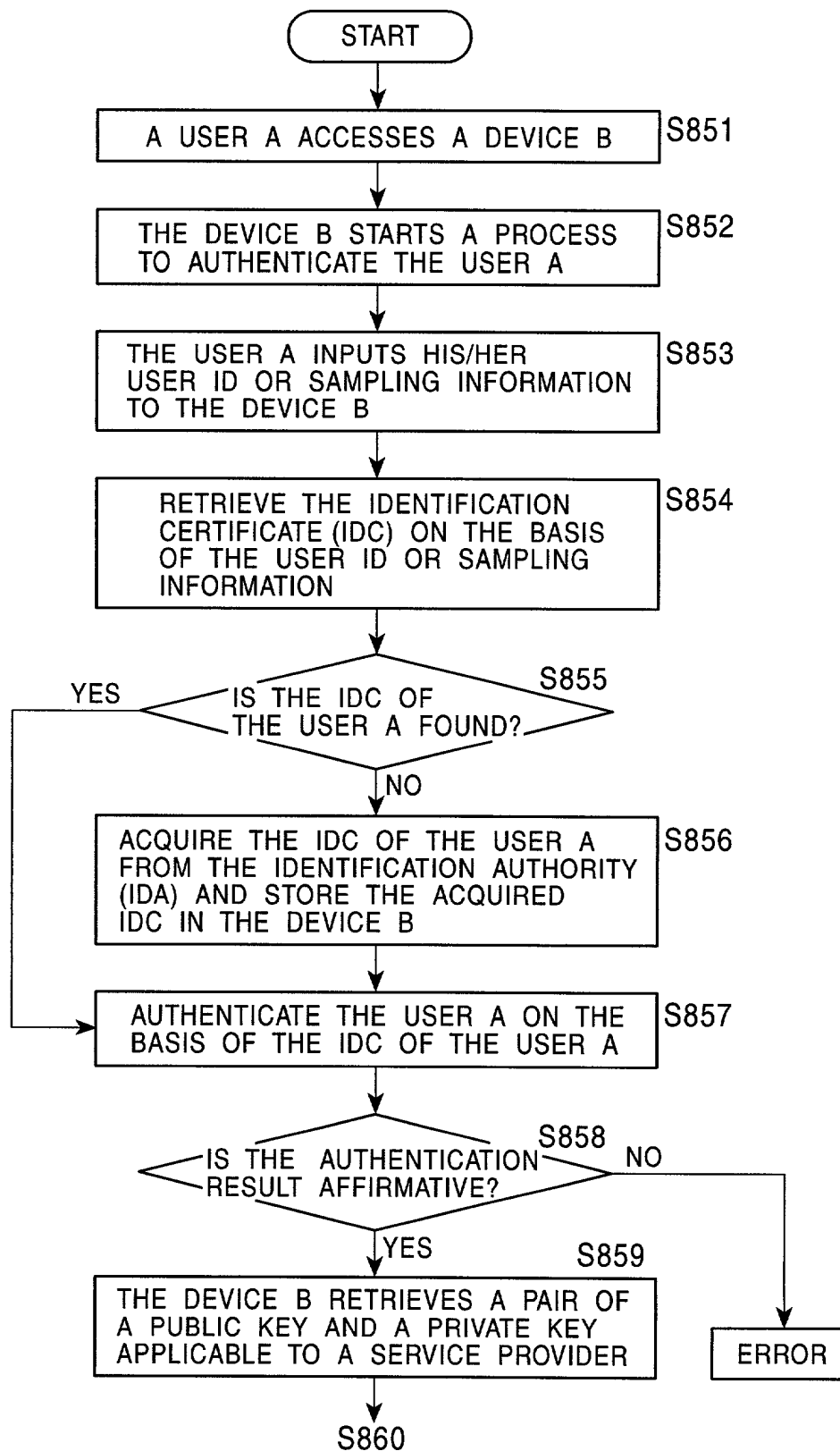


FIG. 78

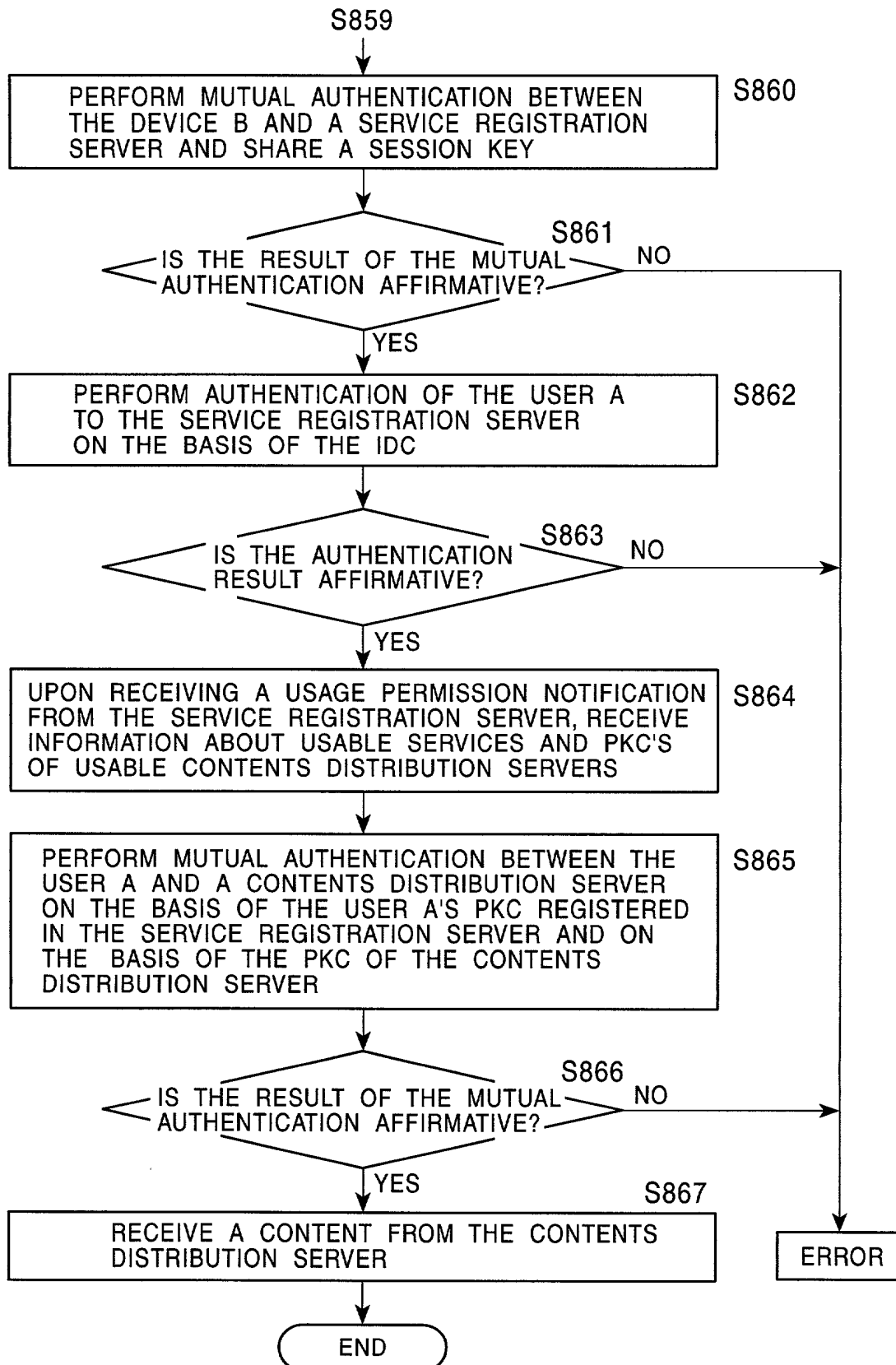




FIG. 79

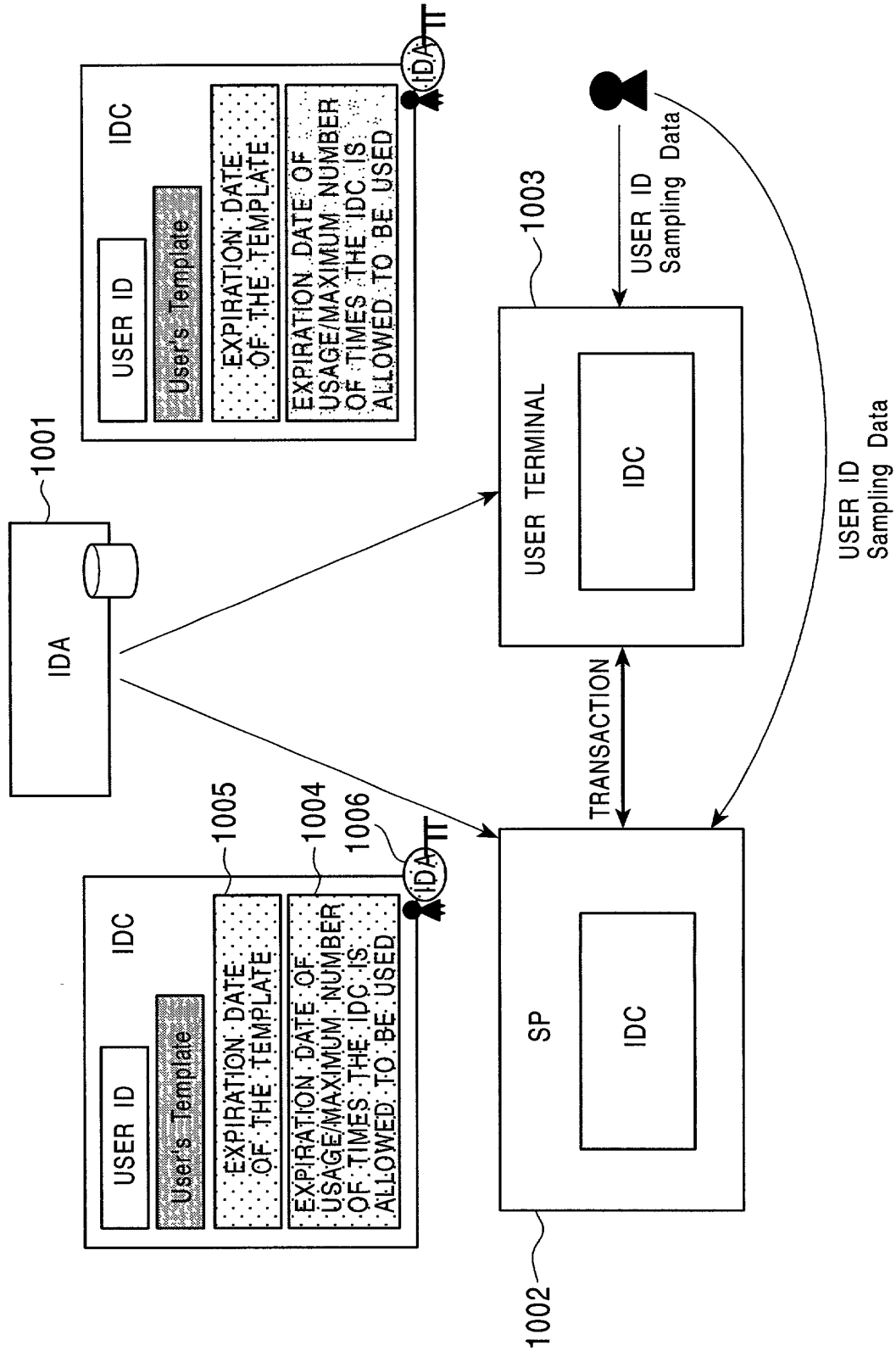


FIG. 80A

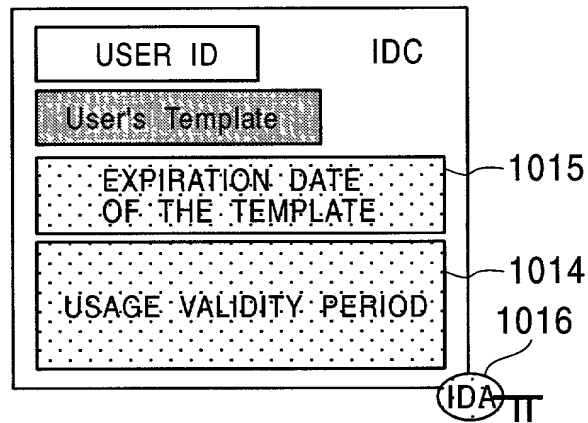


FIG. 80B

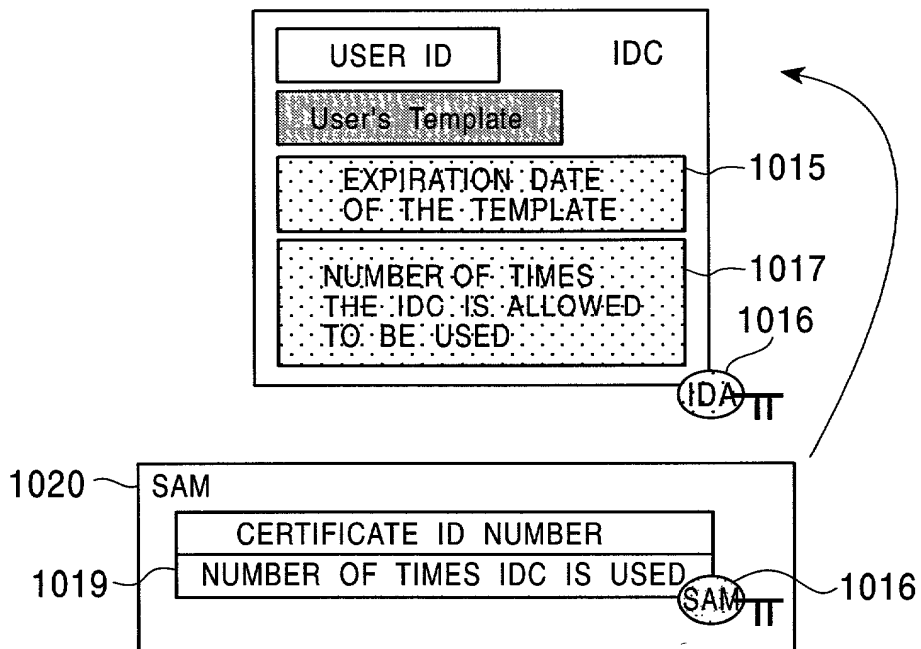


FIG. 81

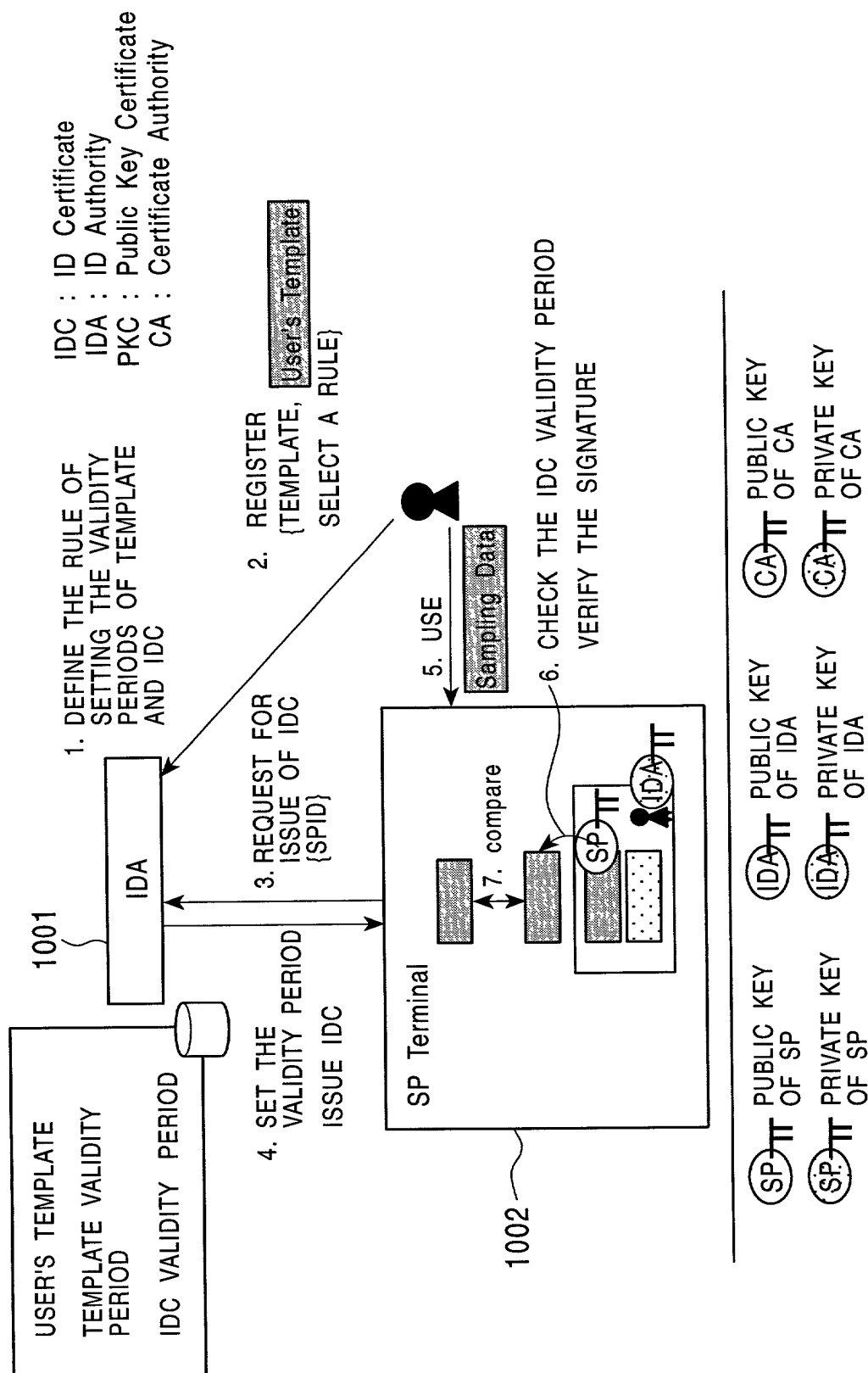


FIG. 82

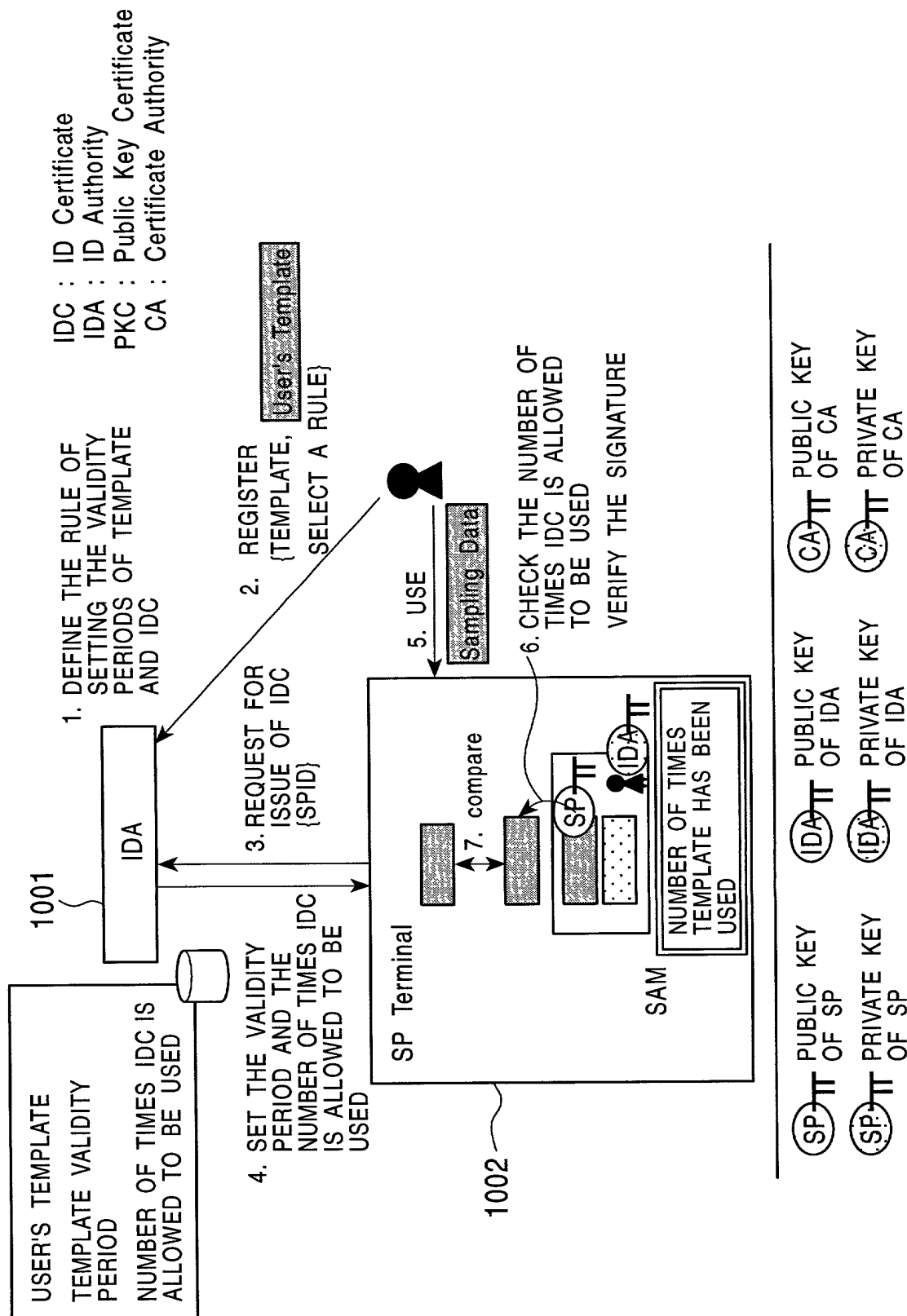


FIG. 83

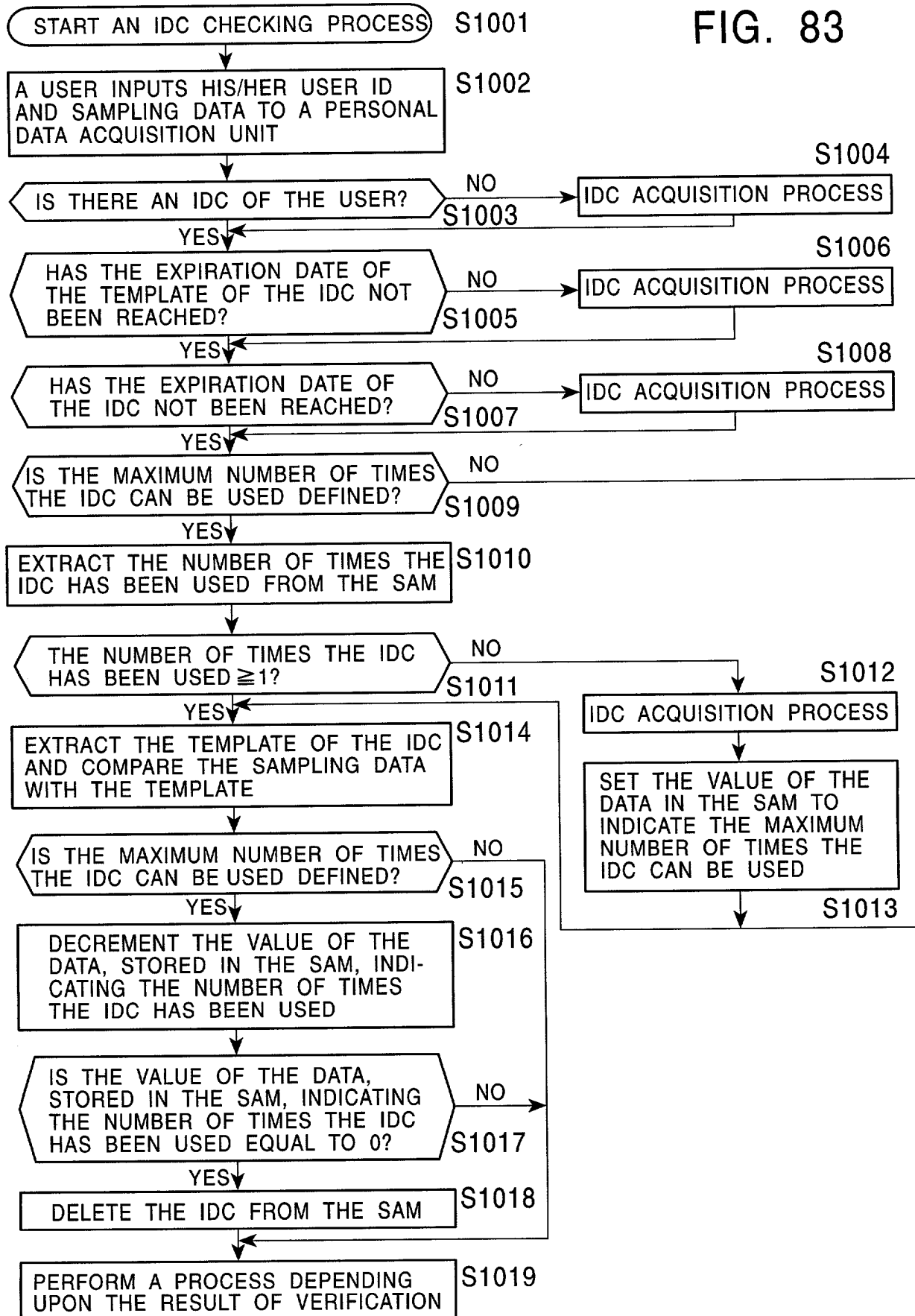


FIG. 84

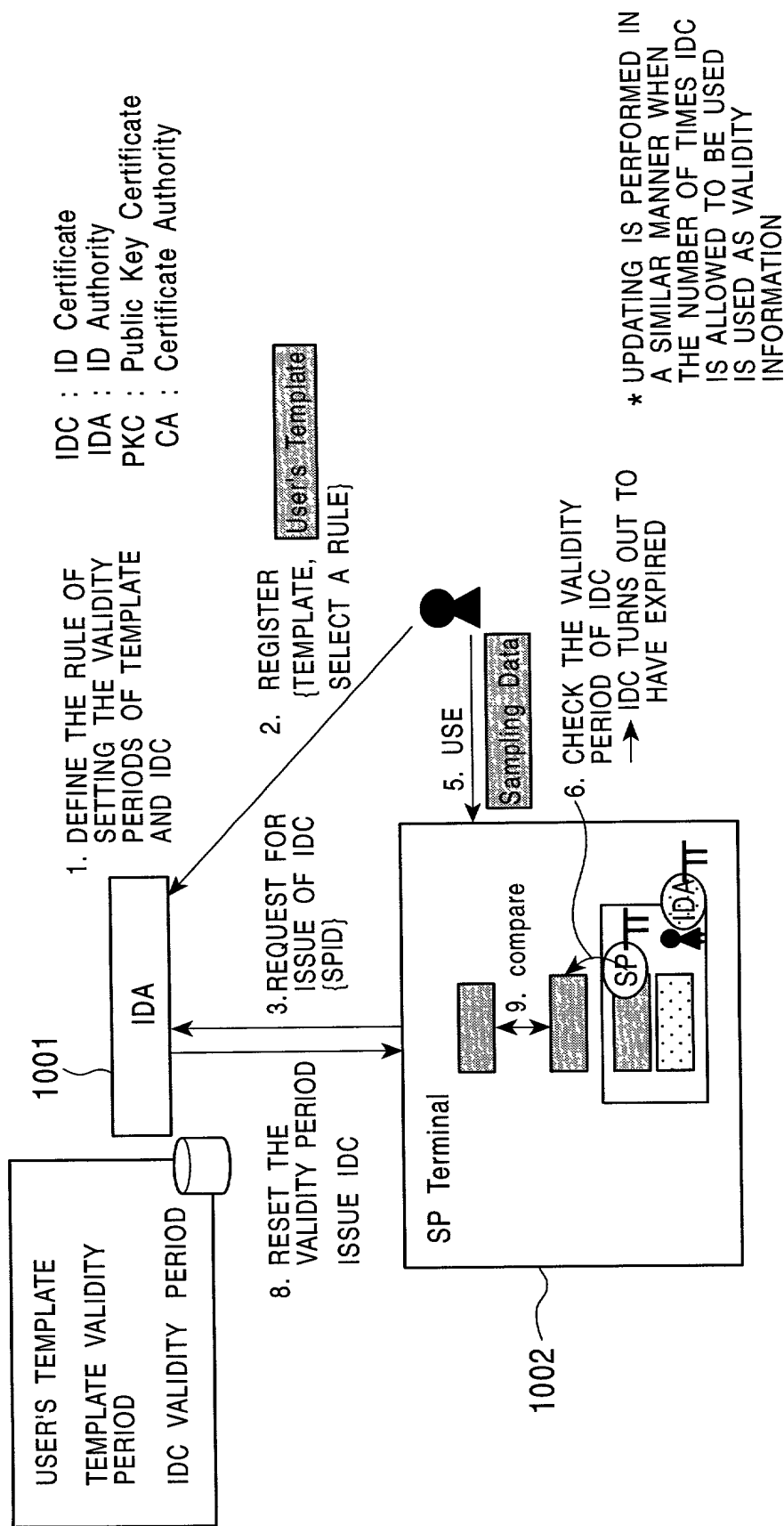


FIG. 85

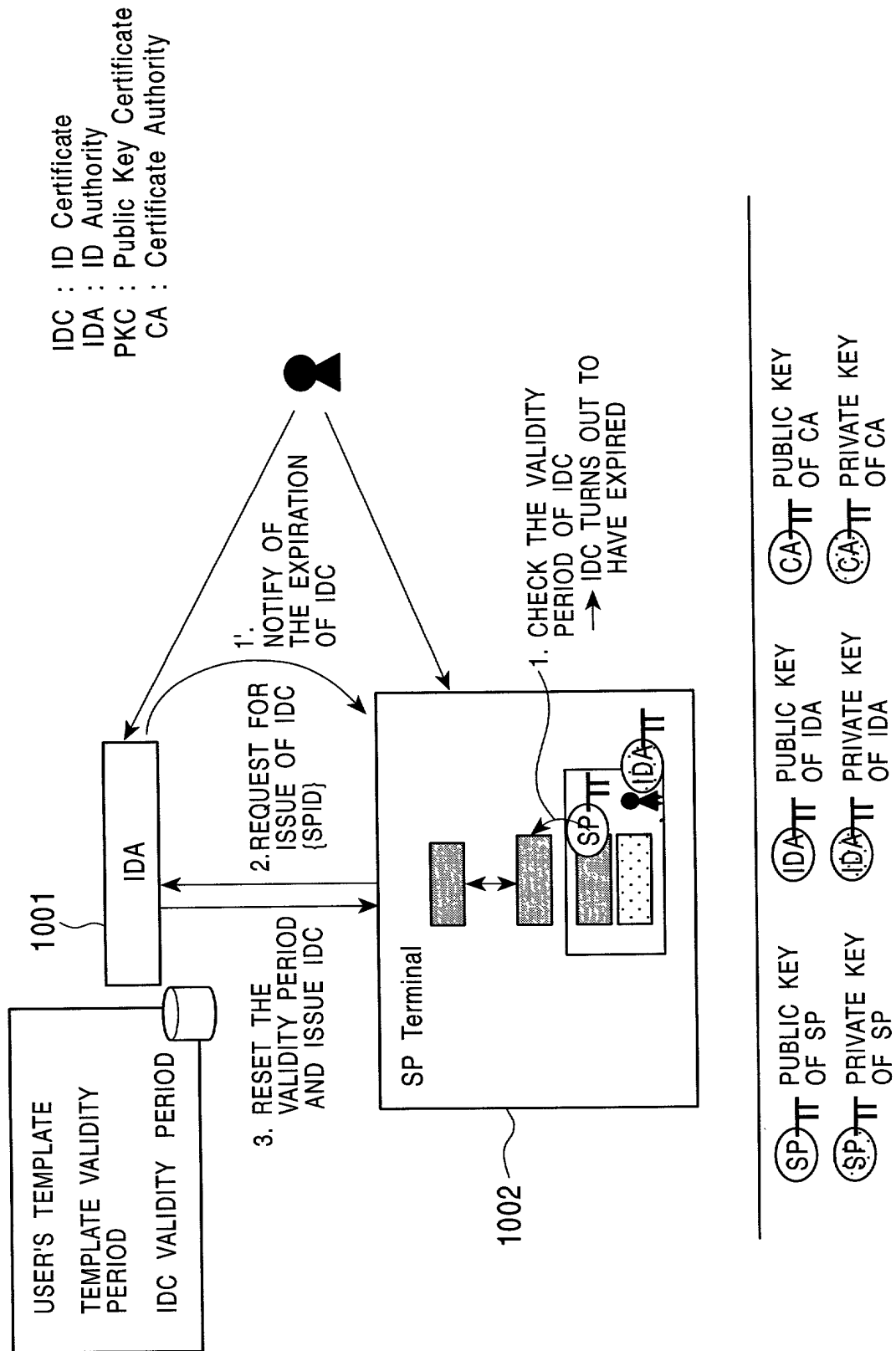


FIG. 86

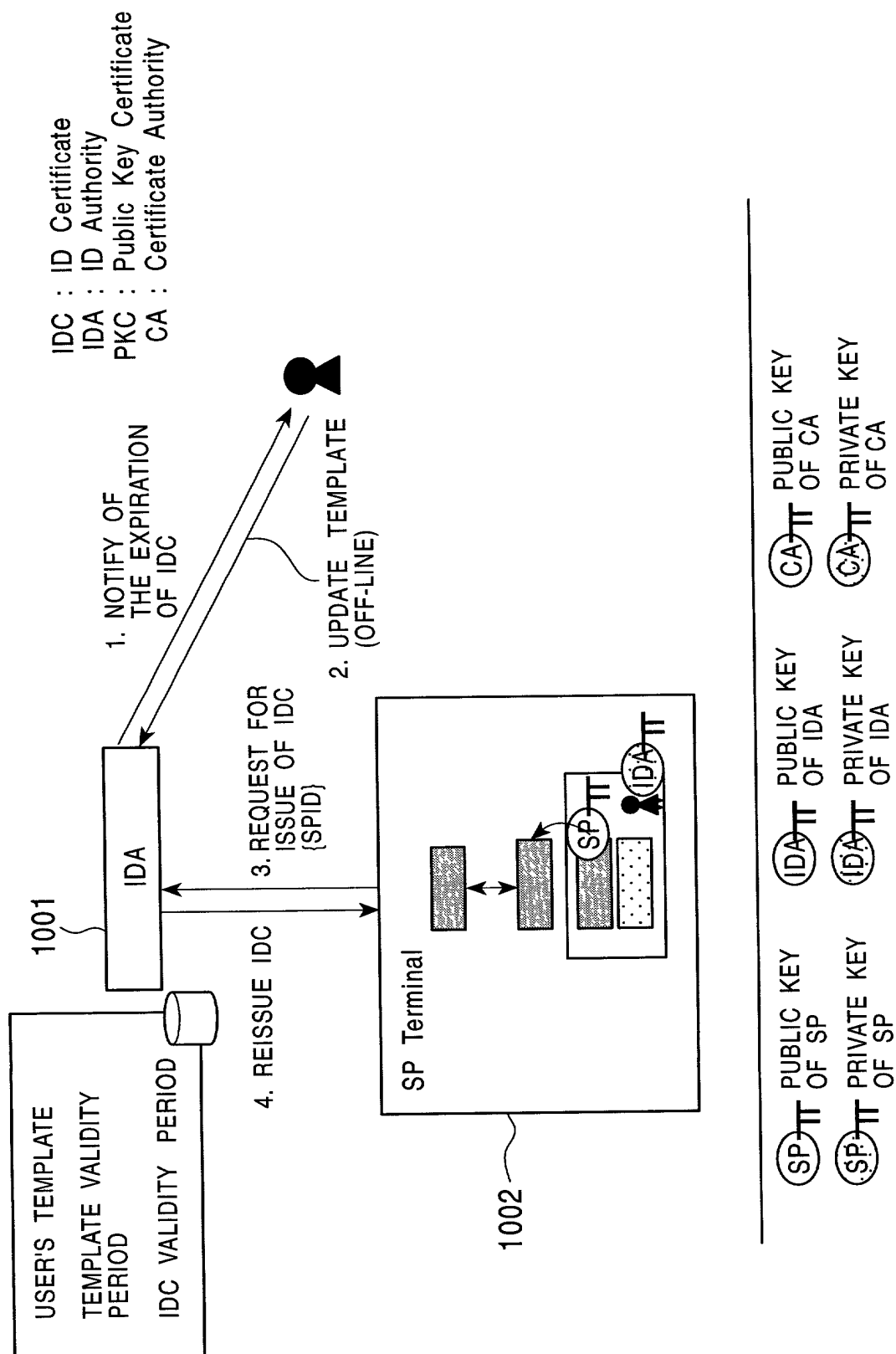




FIG. 87

